Version: 2009-11-30

RCCMD – Multiple Server Shutdown Software

User manual

Limited Warranty

This software and the enclosed materials are provided without warranty of any kind. The entire risk as to software quality, performance of the program, media free of defects, faulty workmanship, incorrect use of the software or UPS, error free documentation and enclosed material is assumed by the user. We do not take any warranty to the correct functions of the software and the security of your system nor files, that might be damaged to due to possibly not correct function of our software. No warranty to correct functions of the software with the operating systems, loss of data or interruption of work processes, other UPS problems or to other errors that may occur out of this combination.

Copyright

The information contained in this manual is non-conditional and may be changed without due notice. The software manufacturer undertakes no obligations with this information. The software described in this brochure is given on the basis of a license contract and an obligation to secrecy (i.e. an obligation not to further publicise the software material). The purchaser may make a single copy of the software material for backup purposes. No parts of this manual may be transferred to third persons, either electronically or mechanically, or by photocopies or similar means, without the express written permission of the software manufacturer.

The UPS-Management software includes a license key for each license. This license is valid for using the UPS service on one server with one UPS and an unlimited number of connected UPSMON-WINDOWS workstations. For operation on several servers a license for every new server is required, disregarding the fact if UPS service runs at that location or if the server is halted by an UPS service via remote command RCCMD. The same regulations are applicable to the use of remote send/receive modules RCCMD and multiserver shutdown under Windows OS, MAC OS and Unix. The service programs are generally delivered as a single license. If there is more than one disk in one package all of them have the same serial number and must not be used for future installations. To use a single CD-ROM for several multiserver shutdown installations you have to purchase additional CD license keys.

Copyright of the European Union is effective (Copyright EU).

Copyright (c) 1995-2009 GENEREX GmbH, Hamburg, Germany.

All rights reserved.

Revision	History	Date
-001	First Release.	10/2008
-011	Update: Function “Sending of a message to all RCCMD clients”	10/2008
-012	Added: RCCMD on Citrix XEN Server	11/2008
-013	RCCMD with SSL	12/2008
-014	Update: UNIX multiple sender configuration	01/2009
-015	Added: Alternative SSL configuration	02/2009
-016	Added: Syntax for switching outputs	03/2009
-017	Added: RCCMD Client as relay station	03/2009
-018	Update: Installation of RCCMD	06/2009
-019	Update: RCCMD InstallAnywhere Installation	07/2009
-020	Added: Silent Installation Windows	08/2009
-021	Added: Grafical RCCMD relay configuration	08/2009
-022	Added: Combined RCCMD Silent Installation and Configuration	10/2009
-023	Added: Silent Installation UNIX	11/2009
-024	Added: Console Installation UNIX	11/2009
-025	Added: RCCMD on ESXi Server 4.x	11/2009
-026	Added: Know How Pool	11/2009

Table of contents

1. What is the RCCMD Software? 5
2. Network Shutdown with RCCMD 5
3. Installation / Configuration of RCCMD for Windows 7
3.1 Installation of RCCMD 7
3.1.1 Silent Installation of the RCCMD Installation 17
3.1.2 RCCMD Silent Installation and Takeover of own Configuration 17
3.2 Testing of the Shutdown.Bat File 18
3.2 Older Installation of RCCMD 20
3.3 Settings of the Authorization of the RCCMD Service 22
3.4 Installation of RCCMD with Redundancy (from RCCMD V3) 25
3.5 RCCMD Client as Relay Station 28
3.6 RCCMD on Windows 95/98 31
3.7 RCCMD for Windows NT/2000/XP/2003/2008 32
3.8 RCCMD with SSL for Windows 33
3.8.1 RCCMD with own SSL certificates 37
3.3.5 Testing the RCCMD connection 37
3.9 Testing the RCCMD 2 connection 38
3.10 RCCMD on NovellNetWare 40
4. RCCMD on UNIX (with graphical interface) 44
4.1 Silent Installation of the RCCMD Installation 51
4.2 Console Installation of the RCCMD Installation 51
4.3 UNIX RCCMD Configuration With CURSES Library 54
4.4 RCCMD Client as Relay Station 67
4.5 RCCMD with SSL for UNIX 67
4.5.1 RCCMD with own SSL certificates 71
5. RCCMD on DEC VMS 72
6. RCCMD on MAC OS 9 74
7. RCCMD on MAC OS 10.X 79
8. RCCMD on Citrix XEN Server 85
9. RCCMD on VMWare ESX Server 3.5.x 86
10. RCCMD on VMWare ESXi Server 4.0.x 87
11. RCCMD AS400-Client 91
Appendix 92
A OpenSSL 92
B Syntax for the switching of the outputs 92
C Know How Pool 93
D Figures 93

1. What is the RCCMD Software?

RCCMD is a network client software, which enables to receive shutdowns or messages from UPS servers like UPSMAN UPS Software, CS121 SNMP Adapters or any other kind of RCCMD capable network-cards of other licenzed partners. RCCMD is the successfulliest multiple server shutdown and messaging tool in the entire UPS world.

2. Network Shutdown with RCCMD

The program RCCMD is designed to execute a command on a remote system in a TCP/IP network. RCCMD works like the Remote Shell (RSH) known in the Unix environment. Inside the UPS-Management Software RCCMD is used to shutdown several servers that are all powered by a single UPS. For this job, one of these computers is configured as UPS-master server.

Install the UPS-Management Software UPSMAN on your UPS server and connect it to the UPS. Alternatively, a SNMP adapter CS-111 or CS-121 can be used for this as well. The other servers are only connected to the UPS power supply, no RS-232 connection is necessary. On these remote systems, install RCCMD (copy the modules) and create a shutdown routine for every system. This shutdown routine may be a batch file, shell script or ncf-file, that contains the down and other commands for this system. After that, add *RCCMD* to the shutdown job or to the EVENT configuration of the computer running as UPS master server.

So now you have a computer in your server network supervising the UPS. The other servers execute RCCMD and wait for the RCCMD signal of the UPS server. If a power failure forces the master computer to shutdown the server-network, the shutdown-job of the UPS-server will start RCCMD. RCCMD now sends the RCCMD-signal to all computers in its list. The computers receive this signal and the installed RCCMD will execute the programmed command.

Please note that it is required to install RCCMD in two different operating ways:

1. as a sending process on the UPS-server,

   (RCCMD –s) (send)

2. as a receiving process (background-process) on the receiving computers.

   (RCCMD –l) (listen)

In contrast to the RSH, RCCMD does not include the command that is to be executed in the sending process, but instead deposits the command with the receiving process. This provides a security advantage in comparison to the RSH. Furthermore the receiving process may check, which computer sends the RCCMD-signal and determines whether to accept it or not.

Attention:

If a name resolution is achieved via DNS, please always use the IP-address (and not the computer name) for a network shutdown with RCCMD. In case the DNS is not available, the network shutdown will not work, if this method is not used.

RCCMD Version 2 or higher

The extended Version of RCCMD is also able to execute commands on remote computers, execute the shutdown batch in the same TCP/IP port 6003, execute an e-mail batch, enable log file entries etc. The RCCMD 2 sender (UPSMAN or CS121 SNMP adapter) sends the corresponding RCCMD signal and the RCCMD 2 client starts the corresponding batch file, which lead to the execution of the net send message.

The initial command will always come from the UPSMAN or CS121 where as the execution will always be on the RCCMD client side.

Example: The CS121 should send a net send (network message) to a Windows NT network. The CS121 can be programmed so that during the event “Powerfail” a “RCCMD message” will be send. The text of the message is configurable by the user.

Upon on receiving the message by the RCCMD 2 client, the client is starting a batch file and sends the net send message. Sender of the message will be the client and initiator is the UPSMAN or CS121.

This way it is possible to send messages, e-mail etc. in the different networks and operating systems, initiated by an UPS alarm.

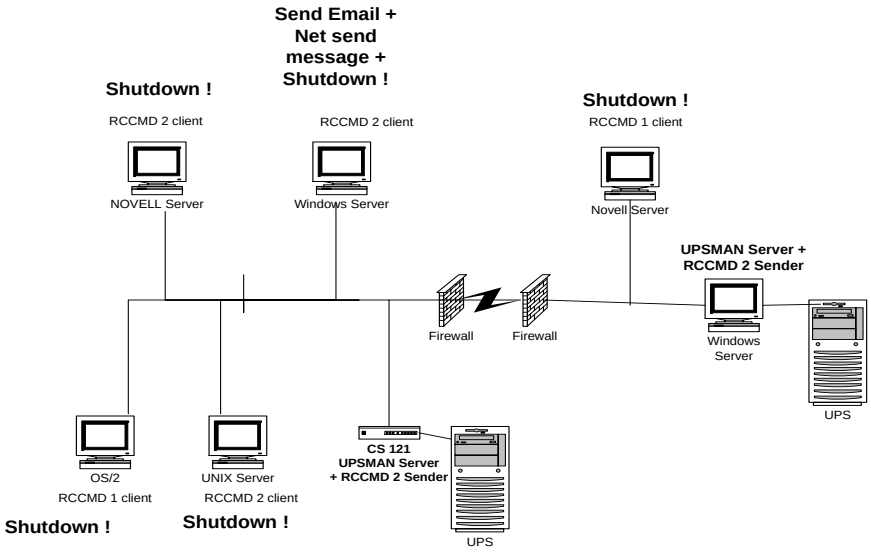


Figure 1 RCCMD and UPSMAN in a network environment

3. Installation / Configuration of RCCMD for Windows

3.1 Installation of RCCMD

Prior of the start, please make sure that you have full administrator rights in order to complete the installation.

Step 1: Put the CD into the CD-ROM drive of your computer or download the software into a specific directory.

Step 2: Please execute the installation program *setup.exe* in order to copy the files to your system and chose a desired setup language.

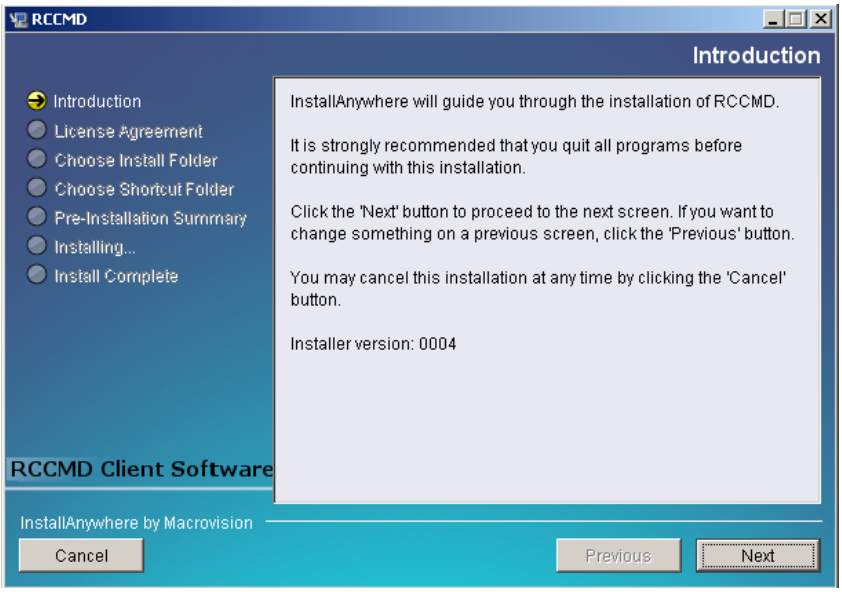

RCCMD
Introduction
Introduction
License Agreement
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere will guide you through the installation of RCCMD.
It is strongly recommended that you quit all programs before continuing with this installation.
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.
You may cancel this installation at any time by clicking the 'Cancel' button.
Installer version: 0004
RCCMD Client Software
InstallAnywhere by Macrovision
Cancel
Previous
Next

Figure 2 Introduction

In the next menue you can see the progress column where the next steps are visible. Click the “NEXT” button to continue.

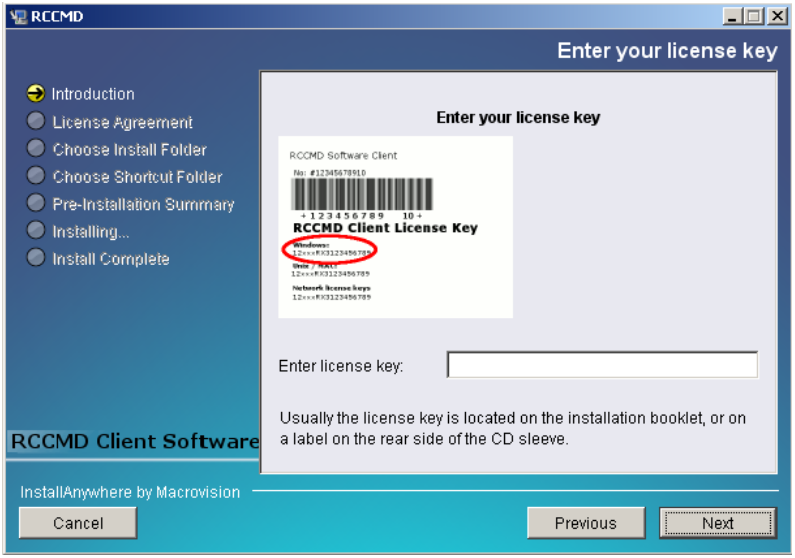


Figure 3 License Key Entry

Step 3: Please enter your license key an choose your corresponding Windows OS from the list. The used license determines, which module can be installed.

Attention: **If you enter a wrong license number at this stage, the RCCMD client software will be set to a 30 day trial version. Please contact your UPS dealer for the full, correct license if it was not with the original CD-ROM.**

You need a special license key for your RCCMD software. You can identify the key with the **"RX3"** in the first part of the license key. Most of the times you need to order the key separately.

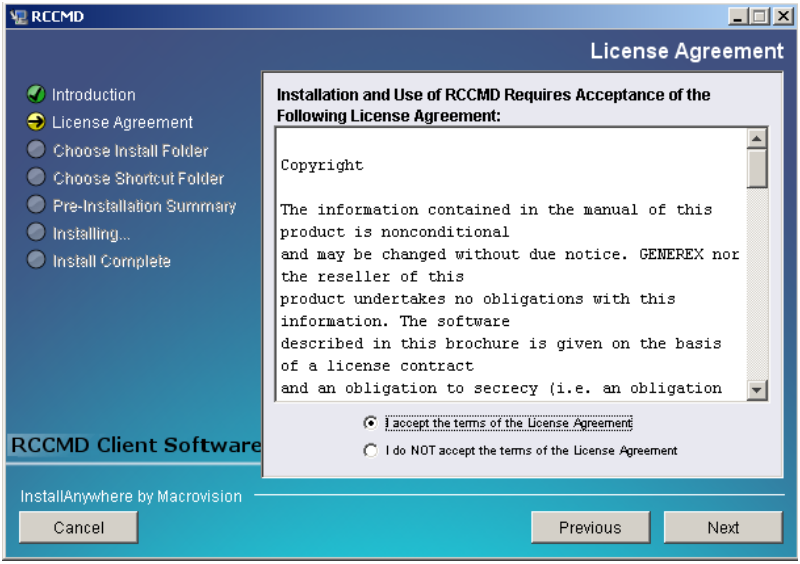

RCCMD
License Agreement
Introduction
License Agreement
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
Installation and Use of RCCMD Requires Acceptance of the Following License Agreement:
Copyright
The information contained in the manual of this product is nonconditional
and may be changed without due notice. GENEREX nor the reseller of this
product undertakes no obligations with this information. The software
described in this brochure is given on the basis of a license contract
and an obligation to secrecy (i.e. an obligation
I accept the terms of the License Agreement
I do NOT accept the terms of the License Agreement
RCCMD Client Software
InstallAnywhere by Macrovision
Cancel
Previous
Next

Figure 4 License Agreement

Read and confirm the license agreement and continue with the “NEXT” button.

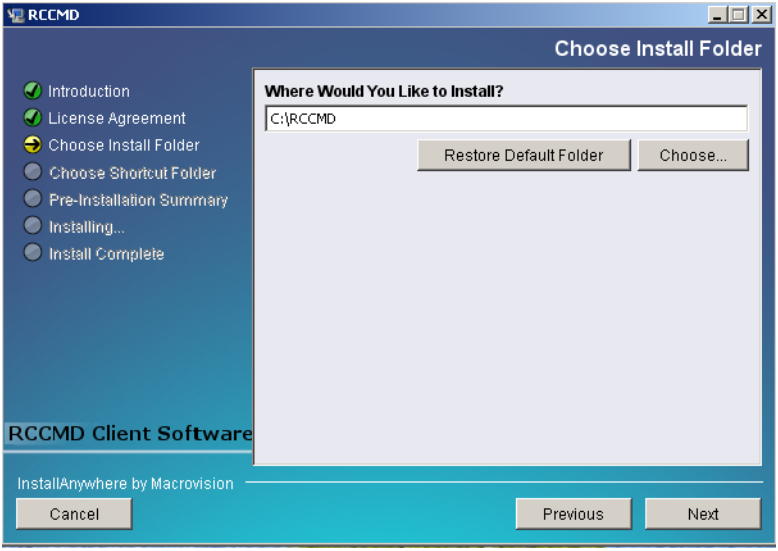


Figure 5 Install Folder Selection

In the next window enter the path where you want to install the software. Default is the subdirectory “UPS” into the program files folder onto the hard disk “C:”.

In next menu you can choose to create a new program group (default) or to choose icons elsewhere or not at all.

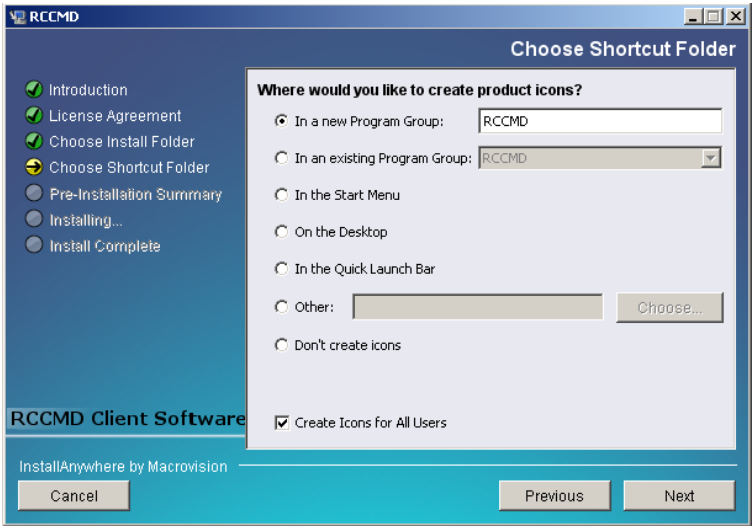


Figure 6 Shortcut Folder Selection

In the next menu you see an overview of your installation and you may now press “Install” to begin.

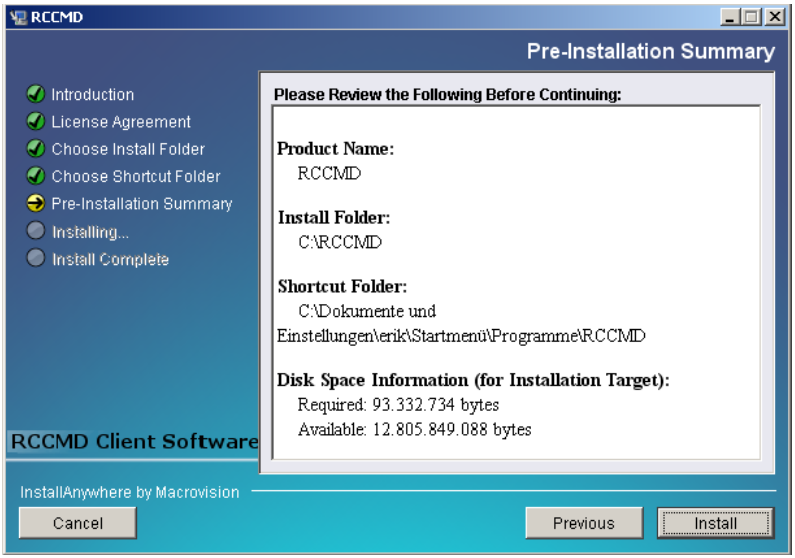


Figure 7 Summary

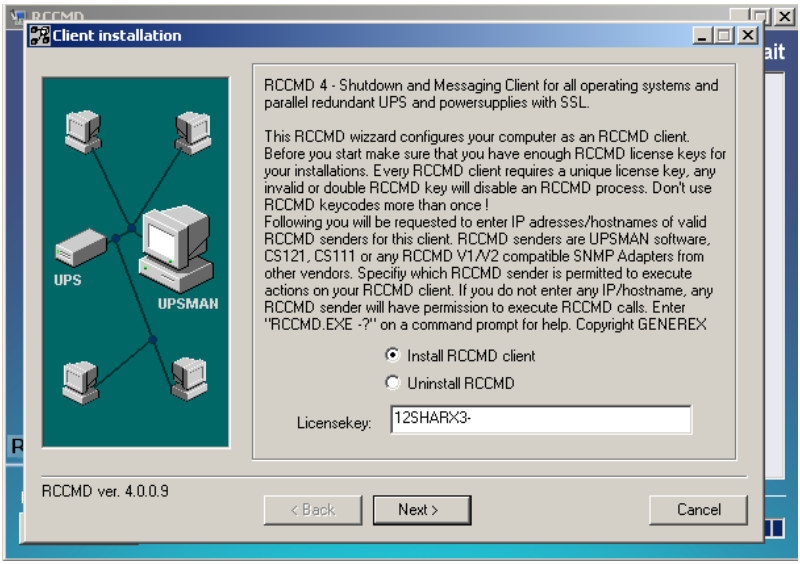

Client installation
RCCMD 4 - Shutdown and Messaging Client for all operating systems and parallel redundant UPS and powersupplies with SSL.
This RCCMD wizzard configures your computer as an RCCMD client. Before you start make sure that you have enough RCCMD license keys for your installations. Every RCCMD client requires a unique license key, any invalid or double RCCMD key will disable an RCCMD process. Don't use RCCMD keycodes more than once !
Following you will be requested to enter IP adresses/hostnames of valid RCCMD senders for this client. RCCMD senders are UPSMAN software, CS121, CS111 or any RCCMD V1/V2 compatible SNMP Adapters from other vendors. Specifiy which RCCMD sender is permitted to execute actions on your RCCMD client. If you do not enter any IP/hostname, any RCCMD sender will have permission to execute RCCMD calls. Enter "RCCMD.EXE -?" on a command prompt for help. Copyright GENEREX
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3-
UPS
UPSMAN
RCCMD ver. 4.0.0.9
< Back
Next >
Cancel

Figure 8 Client Installation

Click the „Next“ button.

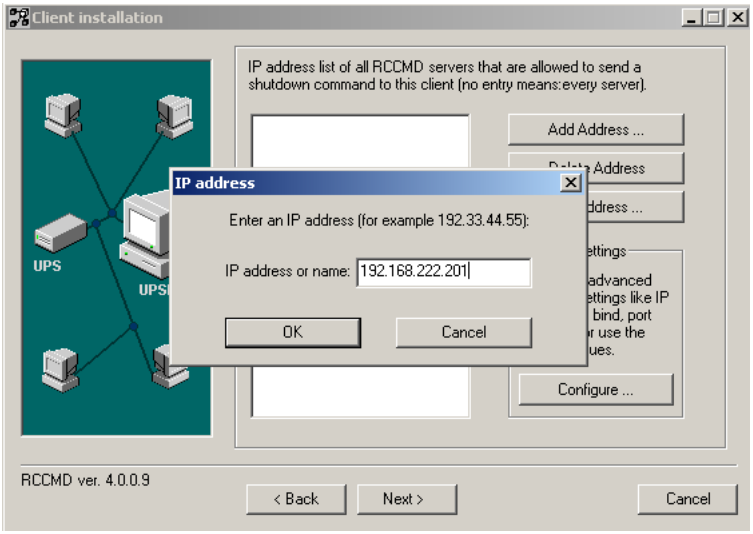


Figure 9 Add IP-Address Window

Step 4: Add the IP address of the RCCMD server, which is allowed to send a shutdown to this client.

Attention:

If you do not enter an address, then every server has the permission to send a shutdown command. If more than one CS121 or rather UPSMAN is existent, thus a redundancy situation, you need to enter more than one address as authorized sender.

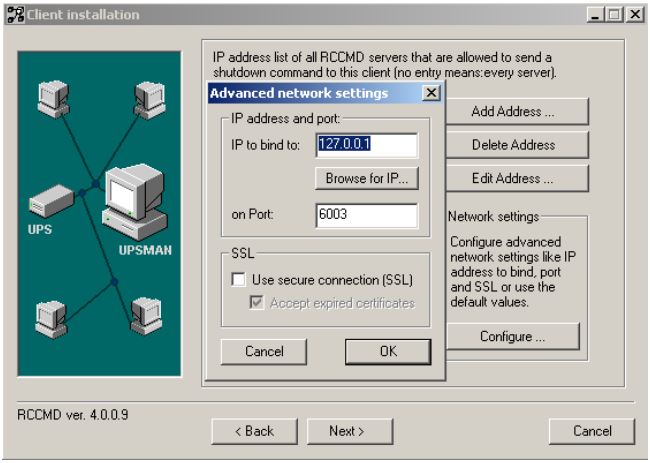


Figure 10 Advanced Network Settings

Step 5: If you want to use the secure connection (SSL), click the “Configure…” button and check the “SSL” box.

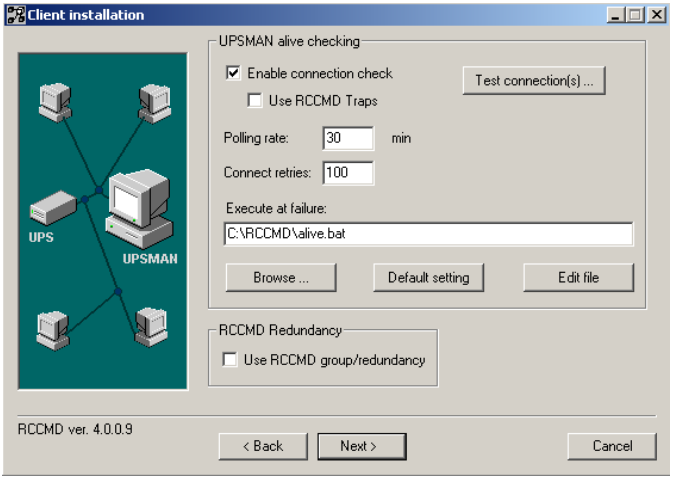


Figure 11 UPSMAN Alive Checking / Redundancy Window

Step 6:

If you want to use the UPSMAN alive checking (recommended), check the “Enable connection check” box. Alive check is a signal, send out to the UPSMAN or CS121 on port 5769 to check if the UPSMAN has still UPS data – or not. If this fails, the scriptfile alive.bat will be executed which causes a messagbox coming up. The polling rate (default 30 min.) defines the polling of the UPSMAN service, connect retries (default 5) means after 5 unsuccessful connection tries an alarm will be triggered.

The function “Use RCCMD Traps” enables UPSMAN/RCCMD/UNMS traps, which show the UPS status as a trap message. If activated it will display a local message when the UPS status of the UPSMAN/RCCMD server changes.

If you click the “Test connection(s)…” button, the UPSMAN alive checking of the entered IP addresses will start (port 5769 will be tested).

If you click the „Browse...“ button, you will get a selection of the default batch files.

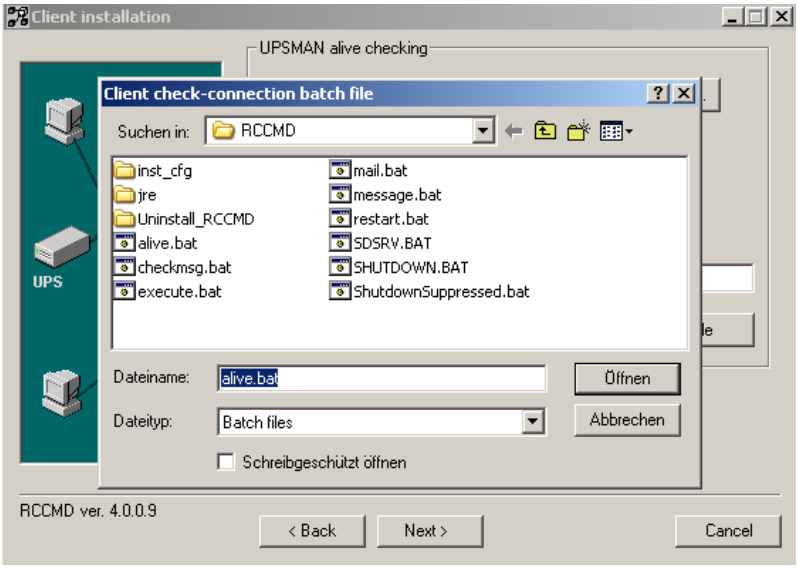


Figure 12 Client Check Connection Batch File Window

If you click the „Default setting“ button, you will get back to the default batchfile (alive.bat).

At the failure of the UPSMAN alive checking, you can define an executing file or edit the default file “alive.bat”: (file contents as follows)

@echo off

rem * "messagetext" %1 == ip-address, %2 == date, %3 == time *** "title" -c counter for beeps**

start /b msg.exe "Check Upsman %1 failed (%2, %3)" "ATTENTION RCCMD:" -c:1

Click the “Next” button.

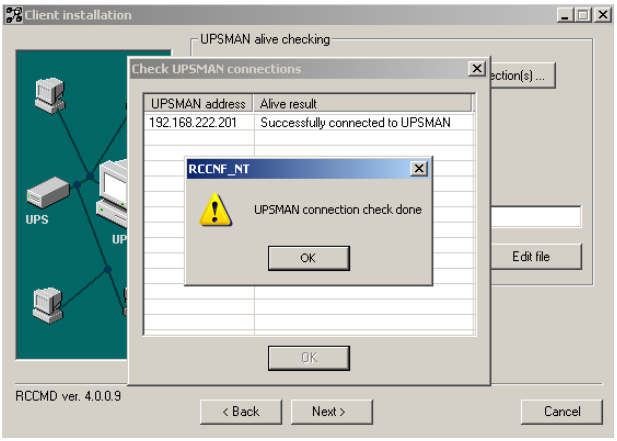


Figure 13 Check UPSMAN Connections Window

Step 7: You can configure the log file size and edit the executing bat files in this installation window.

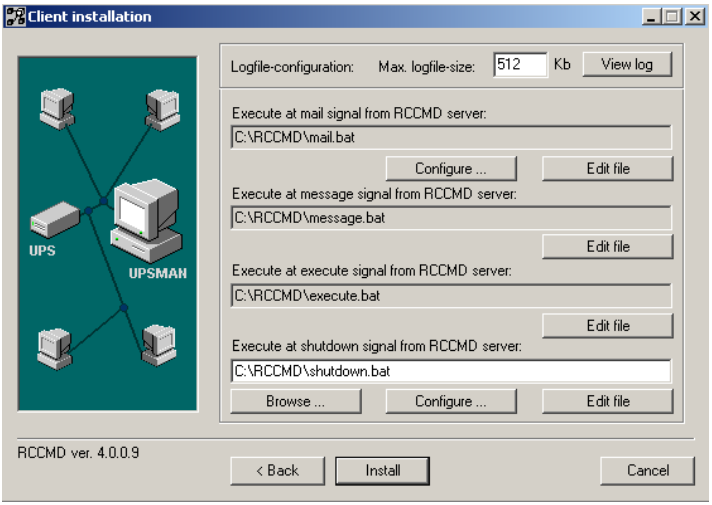


Figure 14 Configure / Edit Bat Files

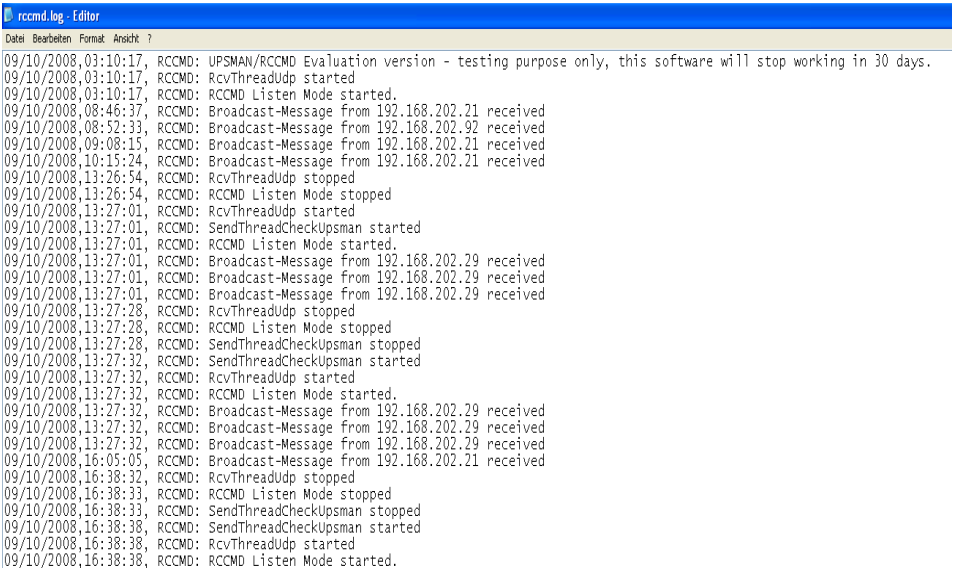

rccmd.log - Editor
Datei Bearbeiten Format Ansicht ?
09/10/2008,03:10:17, RCCMD: UPSMAN/RCCMD Evaluation version - testing purpose only, this software will stop working in 30 days.
09/10/2008,03:10:17, RCCMD: RcvThreadUdp started
09/10/2008,03:10:17, RCCMD: RCCMD Listen Mode started.
09/10/2008,08:46:37, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,08:52:33, RCCMD: Broadcast-Message from 192.168.202.92 received
09/10/2008,09:08:15, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,10:15:24, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,13:26:54, RCCMD: RcvThreadUdp stopped
09/10/2008,13:26:54, RCCMD: RCCMD Listen Mode stopped
09/10/2008,13:27:01, RCCMD: RcvThreadUdp started
09/10/2008,13:27:01, RCCMD: SendThreadCheckUpsman started
09/10/2008,13:27:01, RCCMD: RCCMD Listen Mode started.
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:01, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:28, RCCMD: RcvThreadUdp stopped
09/10/2008,13:27:28, RCCMD: RCCMD Listen Mode stopped
09/10/2008,13:27:28, RCCMD: SendThreadCheckUpsman stopped
09/10/2008,13:27:32, RCCMD: SendThreadCheckUpsman started
09/10/2008,13:27:32, RCCMD: RcvThreadUdp started
09/10/2008,13:27:32, RCCMD: RCCMD Listen Mode started.
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,13:27:32, RCCMD: Broadcast-Message from 192.168.202.29 received
09/10/2008,16:05:05, RCCMD: Broadcast-Message from 192.168.202.21 received
09/10/2008,16:38:32, RCCMD: RcvThreadUdp stopped
09/10/2008,16:38:33, RCCMD: RCCMD Listen Mode stopped
09/10/2008,16:38:33, RCCMD: SendThreadCheckUpsman stopped
09/10/2008,16:38:38, RCCMD: SendThreadCheckUpsman started
09/10/2008,16:38:38, RCCMD: RcvThreadUdp started
09/10/2008,16:38:38, RCCMD: RCCMD Listen Mode started.

Figure 15 RCCMD Log File

You can configure the shutdown sequence:

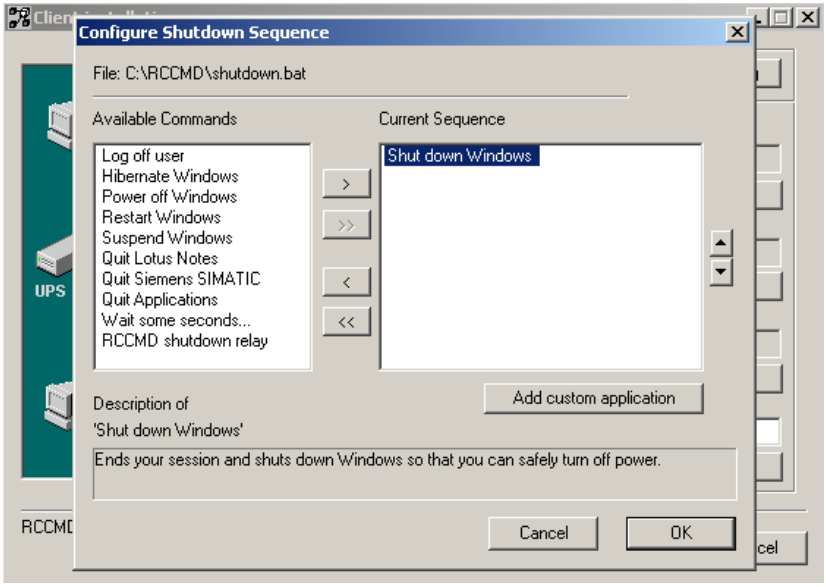


Figure 16 RCCMD Shutdown Sequence Configuration

The following commands are available for the shutdown sequence configuration:

ATTENTION: **The shutdown sequence will be executed from top to down. The "Shutdown Windows" command should be at the bottom, because after the execution of the shutdown, no other commands will be executed.**

Log off user: Ends your session, leaving the workstation on full power.

Hibernate Windows: Hibernates your session, the content of the RAM will be written on hard disk.

Power off Windows: Ends your session, shuts down Windows and turns off the power.

Restart Windows: Ends your session, shuts down Windows and restarts Windows.

Suspend Windows: Suspends your session, the content of the RAM will NOT be written on hard disk.

Quit Lotus Notes: Closes Lotus Notes prior of the shutdown of Windows. Please configure a "Wait" delay after this command.

Quit Siemens SIMATIC: Closes WIN CC Database prior of the shutdown of Windows. Please configure a "Wait" delay after this command.

Quit applications: Closes all applications prior of the shutdown of Windows.

Wait some seconds…: Waits a duration in seconds until the next command will be executed.

RCCMD shutdown relay: Relays RCCMD shutdown command to another workstation. Enter the IP address or the hostname of the remote station you want to shutdown.

Shut down Windows: Ends your session and shuts down Windows, so that you can safely turn off the power.

The default shutdown.bat content is as follows:

rem created by setup

@echo off

set path=C:\WINDOWS\;C:\WINDOWS\system32\;C:\RCCMD

ExitWin.exe shutdown force

@cls

3.1.1 Silent Installation of the RCCMD Installation

The RCCMD Software provides a silent installation, but it is required to enter some settings into the “Installer.Properties” file.

```
## This file provides Values to alter the behaviour of the installer.
## You can preset Values for some internal Variables.
## For the installer to find and use this file it is necessary to either rename
##  this file or pass a parameter to the installer when calling it.
##
## If this file is called 'installer.properties' or has the same name as the
##  installer, e.g. 'install_RCCMD.properties' then the installer should
##  automatically use this file.
##
## To call the installer with a parameter providing a properties file, the
##  installer need the parameter '-f' in this case the command line call looks
##  somewhat like this: "install_RCCMD.exe -f silent-installer.properties".
##
## To set the installer User Interface without providing the variable in the
##  properties file, the parameter '-i' can be used.
##  E.g. "install_RCCMD.exe -i silent"
##  The interface options are "silent,gui,console" the gui option is default.

## This will set the User Interface of the installer
#INSTALLER_UI=silent

## This presets the Licensekey. This value is necessary for a silent
##  installation, because there is no other way to pass this information to
##  the installer.
#GXLICENSEKEY=

## The Dialogbutton variable contains the answer to the pop-up questions whether
##  the RCCMD should be started at system boot and wether it should be started now.
##  the value '0' resembles the answer 'Yes' the value '1' (default) corresponds
##  to 'no'.
#CHOSEN_DIALOG_BUTTON=0

## Select the language for the installed version of RCCMD by setting the
##  INST_LANG variable to the desired country-code
##  (e.g.: el,en,es,de,fr,he,it,ja,ko,pt,ru,tr,zh_cn).
#INST_LANG=en
```

Figure 17 Content of the “installer.properties”

It is required to remove the hash mark prior of the variable `INSTALLER_UI=silent`. In addition the setting of the license key is required behind the variable `GXLICENSEKEY=`.

3.1.2 RCCMD Silent Installation and Takeover of own Configuration

After you have finished the edition of the “installer.properties” file, it is possible to create an own RCCMD configuration and to “silent” install.Thereto it is required to execute the RCCMD configuration manually once. Then export this configuration out of the registry into a file as follows:

- Click the right mouse button on “Parameters” into the directory HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rccmd, select “Export” and save the file with the name “rccmd.reg” as “WIN95/NT4 Registration File”.

- Store the file “rccmd.reg” into the directory, where the RCCMD-Installer packet is located.
- Open the file “rccmd.reg” with an editor and delete the complete line, which contains the license key.
- Create a new Windows batch-file (*.bat) with an editor, e. g. with the name “InstalAndConfigRCCMD.bat”, which should look like as follows:

```
@echo off
cls
echo *** Installation of RCCMD, please wait... ***
installRCCMD.exe
echo *** Importing RCCMD configuration file ***
regedit.exe -s rccmd.reg
echo Ready
```

- Now you can start a combined RCCMD silent installation and configuration via executing of your Windows batch-file “InstallAndConfigRCCMD.bat”.

3.2 Testing of the Shutdown.Bat File

We recommend to test the edited shutdown.bat file. The shutdown program EXITWIN.EXE is predefined. Just enter Exitwin.exe -? in the RCCMD directory for syntax help for this shutdown tool. You may use also your own shutdown tool or any other which we provide with this software.

ATTENTION: **If your configuration works fine in the DEBUG mode, does not necessaryly mean that it works also with the RCCMD as NT service. Please ensure that the RCCMD as service has been started in a user account with administrative rights, otherwise it may happen that only non-restrictive programs may be executed (like notepad.exe) but no Shutdown. (This will result in the NT error message ”Adjust Token Privileges failed”.) If a program has in fact started or not can be seen in Taskmanager window (ALT+CTRL+DEL), because a service does not a started program in the current user session due to non-interactive transaction with the desktop.**

The full command syntax for the NT consol for RCCMD in <Listen mode>:

rccmd [–debug] -l [-a IP adress] [–h hostname] [-p port] "command"

The command can be either a program or a path for another batchfile on this workstation. The command file should be given with full path. The -p port option can be included if you want to start RCCMD more than once at a single workstation to proceed different commands for different events. The default port number is 6003, use any other availabe port number for different RCCMD commands.

RCCMD in the send mode:

rccmd [–debug] -s [-a IP adress] [-h hostname] [-p port]

This command is regularly used in the batchfile of the sender (shutdown.bat) and sends a "ping" to the computers IP adress or hostname. If this ”ping” has been answered, the next command RCCMD –s may be executed, etc.

When you have finished the edition of the bat files, click the “Install” button.

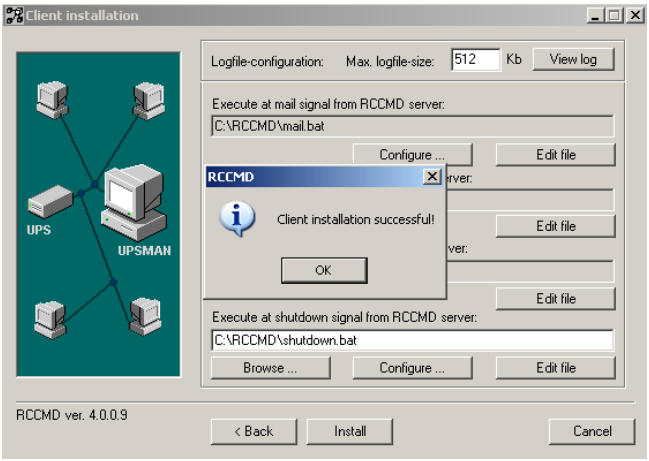


Figure 18 Client Installation successful Window

RCCMD is now running as Service with automatic startup. To configure the automatic start of RCCMD use administrative rights and control panel, service to change the settings.

IMPORTANT: RCCMD as service with local desktop interactions is permitted to execute local shutdowns – for this action no user rights – except administrative rights – are required. But for any user specific actions, e. g. starting a net send message or any other command – the RCCMD may need extra rights! These rights have to configured in the Control panel, services.

Sending of a message to all RCCMD clients

To send a message to all RCCMD clients, please use the following syntax:

rccmd –se “MSG_TEXT ups_says_hello_world” –a 192.9.200.255

The RCCMD client, which should receive this message, need to get the entry of the ip-address of the RCCMD sender or rather the list should be empty. The CS121 is not able to send UDP broadcasts, so you have to enter the above mentioned syntax into the RCCMD client. The client will operate as relay station and will forward the message. It is no problem to send the message from a Windows-, UNIX- or MAC OS RCCMD sender.

3.2 Older Installation of RCCMD

Prior of the start, please make sure that you have full administrator rights in order to complete the installation.

Step 1:	Put the CD into the CD-ROM drive of your computer or download the software into a specific directory.
Step 2:	Please execute the installation program *setup.exe* in order to copy the files to your system and chose a desired setup language.
Step 3:	Please enter your license key an choose your corresponding Windows OS from the list. The used license determines, which module can be installed.

Attention: **If you enter a wrong license number at this stage, the RCCMD client software will be set to a 30 day trial version. Please contact your UPS dealer for the full, correct license if it was not with the original CD-ROM.**

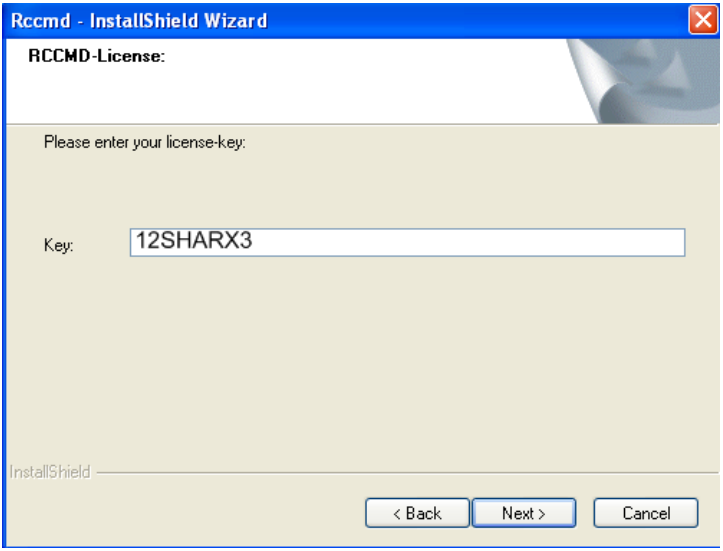


Figure 19 Enter your License Key

You need a special license key for your RCCMD software. You can identify the key with the **"RX3"** in the first part of the license key. Most of the times you need to order the key separately.

Step 4: Select the RCCMD Setup Type. "Complete" means, that all programm features will be installed. "Custom" is for advanced users only.

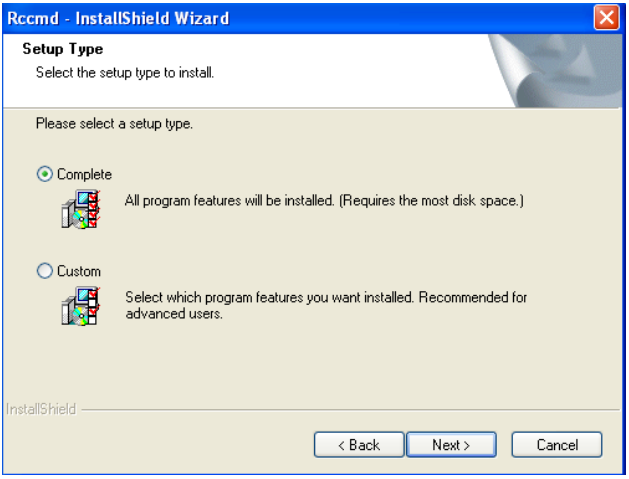

Rccmd - InstallShield Wizard
Setup Type
Select the setup type to install.
Please select a setup type.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Select which program features you want installed. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

Figure 20 RCCMD Setup Type

After you have accepted the agreements and finished the "Install Shield Wizard", you will see the client installation window.

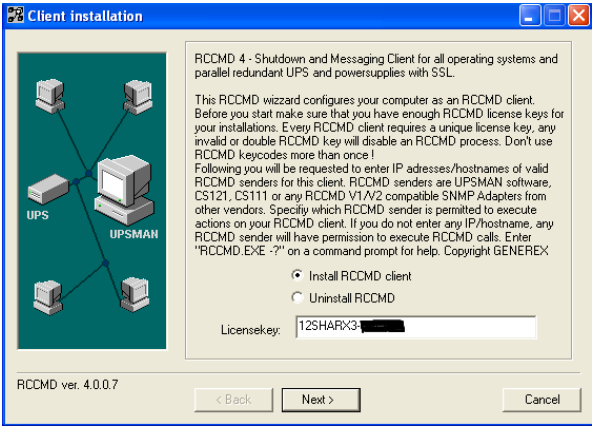

Client installation
UPS
UPSMAN
RCCMD 4 - Shutdown and Messaging Client for all operating systems and parallel redundant UPS and powersupplies with SSL.
This RCCMD wizzard configures your computer as an RCCMD client. Before you start make sure that you have enough RCCMD license keys for your installations. Every RCCMD client requires a unique license key, any invalid or double RCCMD key will disable an RCCMD process. Don't use RCCMD keycodes more than once !
Following you will be requested to enter IP adresses/hostnames of valid RCCMD senders for this client. RCCMD senders are UPSMAN software, CS121, CS111 or any RCCMD V1/V2 compatible SNMP Adapters from other vendors. Specifiy which RCCMD sender is permitted to execute actions on your RCCMD client. If you do not enter any IP/hostname, any RCCMD sender will have permission to execute RCCMD calls. Enter "RCCMD.EXE -?" on a command prompt for help. Copyright GENEREX
Install RCCMD client
Uninstall RCCMD
Licensekey:
12SHARX3-
RCCMD ver. 4.0.0.7
< Back
Next >
Cancel

Figure 21 Client Installation Window

Please take a look on page 11, step 4 for further configuration.

3.3 Settings of the Authorization of the RCCMD Service

Open the menu of the properties window for the RCCMD service (via control panel, administration and services).

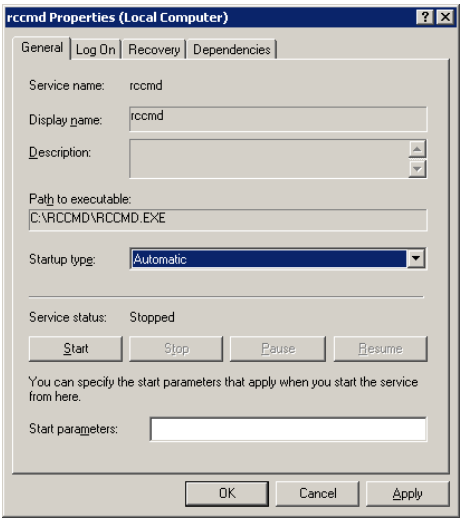


Figure 22 RCCMD Properties Window

Click the “Log On” button on the upper left side.

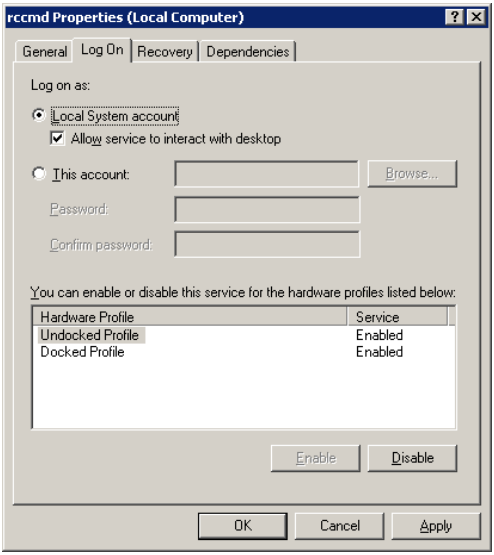


Figure 23 RCCMD Properties Log On Window

Check the “This account” ring and **delete the passwords** and click the “Browse…” button.

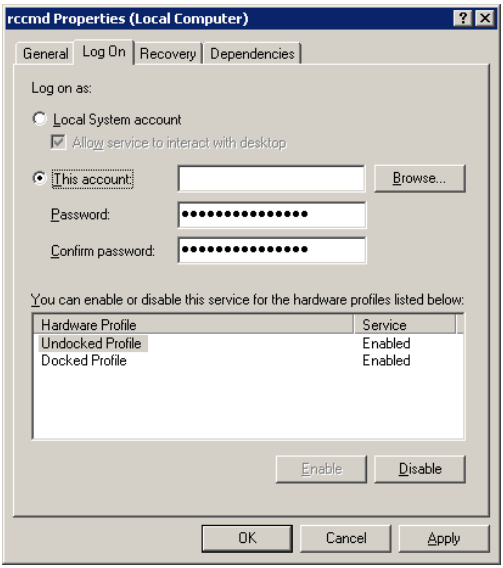


Figure 24 RCCMD Properties Password Confirmation

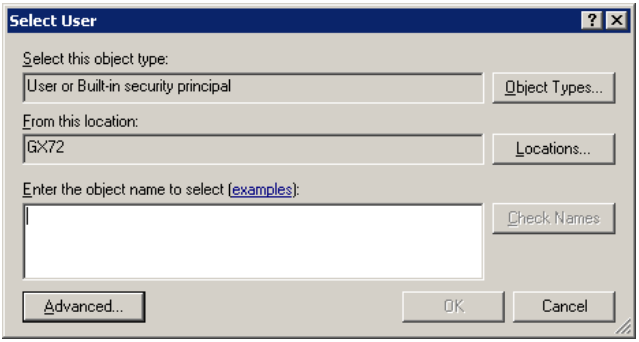


Figure 25 Select User Window

Click the “(examples)” button to select the object name.

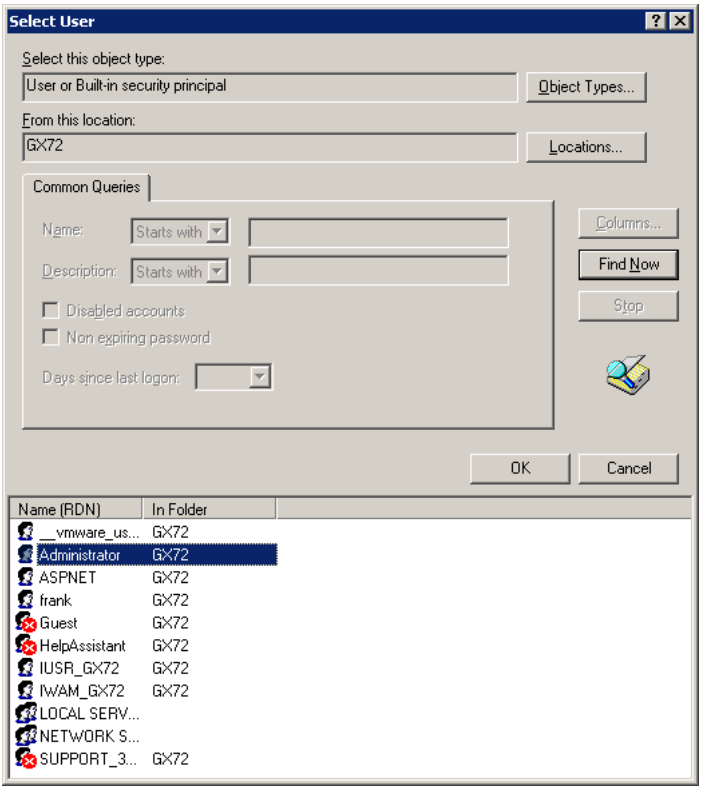


Figure 26 Selection of the Object Name

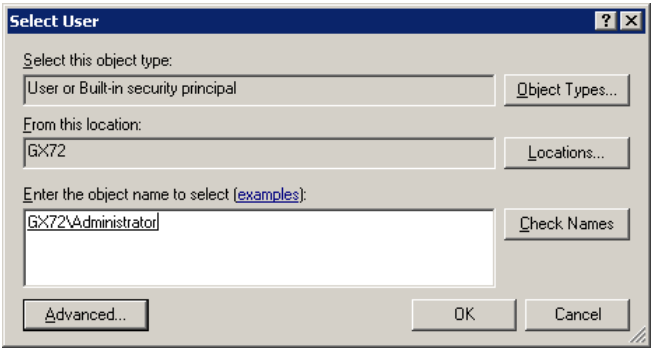


Figure 27 Administrator Selection

Click the “Ok” button and enter the new password twice.

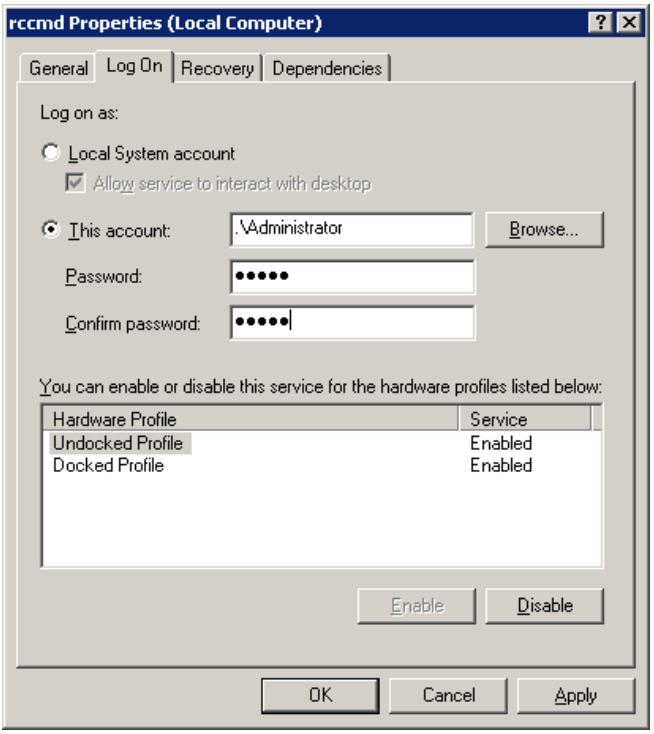


Figure 28 Administrator Password Confirmation

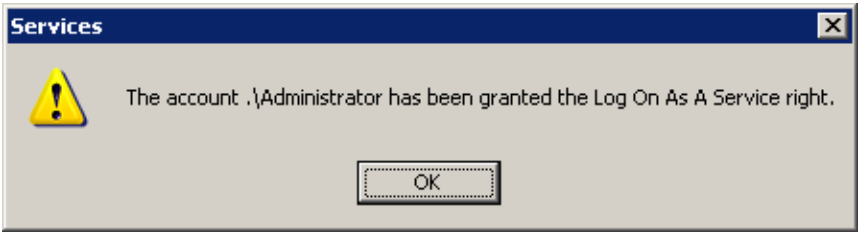


Figure 29 Service Right Info Window

3.4 Installation of RCCMD with Redundancy (from RCCMD V3)

Redundancy is the multiplication of critical components of a system with the intention of increasing the reliability of a system. In many safety-critical-systems, some parts of the control system may be triplicated. An error in one component may then be out-voted by the other two. In a triply redundant system, the system allotted three sub components, which must fail all prior the system fails. Since each one rarely fails, and the sub

components are expected to fail independently, the probability of all three failing is calculated to be extremely small.

At UPS installation RCCMD offers redundancy management functionality as follows:

Every UPS must be equipped with a CS121 or UPSMAN software computer. When ticking the box “use RCCMD group/redundancy” – you are guided to a menue where you can choose which CS121 /UPSMAN are supplying this RCCMD client. E. g. if 4 CS121/UPSMAN are installed into 4 UPS – than each may send a shutdown signal to this RCCMD client.

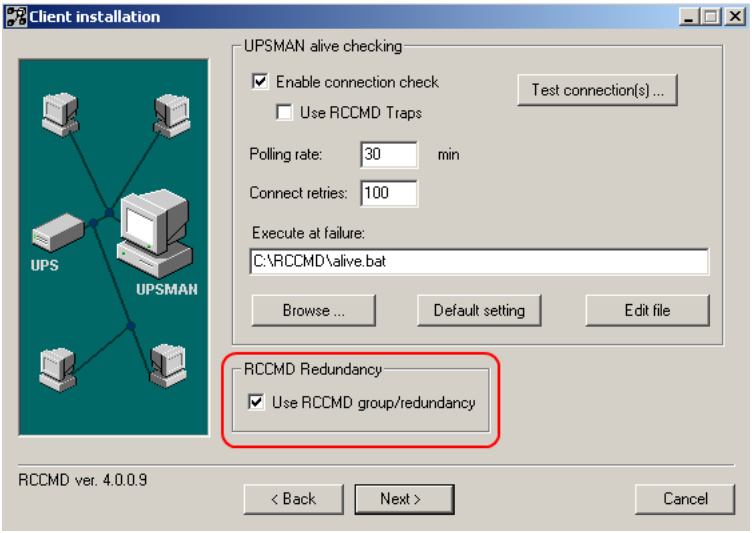


Figure 30 Client Installation RCCMD Redundancy

Click the “Next” button.

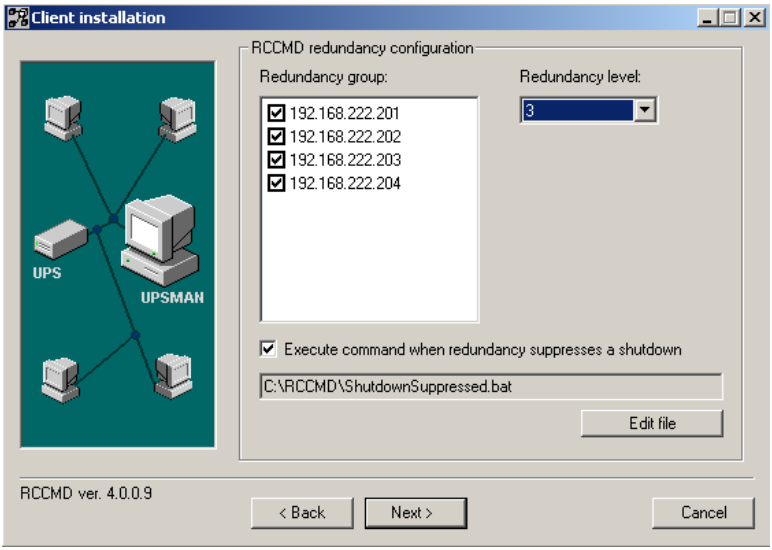


Figure 31 Client Installation RCCMD Redundancy Configuration

The redundancy level defines how many shutdown signals are required to execute the shutdown.bat file. As long as this number is not exceeded, the RCCMD client will react on such a shutdown signal only with a messagebox "Execute command when redundancy suppresses a shutdown" box. This will show a message to inform the user that there has been a shutdown signal from one of the UPS in the group, but since all other UPS are still reading OK – or did not yet send any shutdown, the shutdown is suppressed. 3 shutdown signals would create messages in the above example (redundancy level 3) only, just the 4th signal would initiate the shutdown.

ATTENTION: RCCMD checks the presence of the other group members, prior of the sending of the shutdown-suppressed message! Are the members not reachable, e. g. because of a lost network connection, RCCMD will send the shutdown signal immediately!

Content of this messagebox file "ShutdownSuppressed.bat":

@echo off

start /b msg.exe -c:3

"Attention ! RCCMD Shutdown Signal received. Execution suppressed because of redundancy configuration. Please verify the status of the redundant UPS before you continue to work. NOTE: If the RCCMD shutdown sender problem has been solved, please stop/restart RCCMD service to reset the system. If you do not restart RCCMD service the shutdown is still pending and will be activated if another RCCMD signal arrives !"

When this message box appears the RCCMD client is waiting for more shutdown signals to come until the redundancy level is reached. If this is the case (in the 0065ample above 3 shutdown signals must be send – than the 4tzh signal triggers the shutdown) – than finally the shutdown.bat file is executed an this RCCMD clients goes down.

Attention: If the shutdown is suppressed, and the problem on the UPS side is solved, you MUST NOT forget to restart the RCCMD service to reset the alarm situation ! If you forget to restart RCCMD the software will remember the alarm situation so that in case another signal is send, an immediate shutdown is started. So please restart RCCMD (or your computer) after the UPS problem has been solved.

3.5 RCCMD Client as Relay Station

In order to reach a bigger number of RCCMD receivers, the CS121 adapter needs to be operated as relay station. The receiver will be configured so that it will receive a RCCMD signal and this signal will be used to start a batch file, which then starts even more RCCMD sender signals. This workstation is then sender and receiver at the same time and is therefore an important link in the UPS monitoring chain. Generally the useage of a RCCMD client as a relay station makes the management of several 100 RCCMD clients far easier than configuring this via the Web-interface of the CS121. Additionally, all Web-browser event configurations have a certain limitation so that it is required to use the relay function, if the number of jobs exceed 50 per event at the CS121 HW 131, at older CS121 adapters even earlier.

See the following script, which lets the RCCMD-client act as relay station:

```
@ECHO off
REM --- Created by RCCMD configuration ---
SET path=C:\WINDOWS;C:\WINDOWS\system32\;C:\RCCMD
SET path=%path%;C:RCCMD\
# RELAY RCCMD
# This batch will send RCCMD shutdown calls to the IP addresses listed below
# At the end of the batch this computer will initiate the local shutdown
rccmd -s -a 192.168.200.2
rccmd -s -a 192.168.200.3
rccmd -s -a 192.168.200.4
rccmd -s -a 192.168.200.5
rccmd -s -a 192.168.200.6
rccmd -s -a 192.168.200.7
# to be continued...
#
# local shutdown
ExitWin.exe shutdown force
@CLS
```

Figure 32 Example: Batch File RCCMD act as Relay Station

The RCCMD Version 4.0.1.0 or higher provides a grafical configuration of the RCCMD relay function.

Click the “Configure…” button.

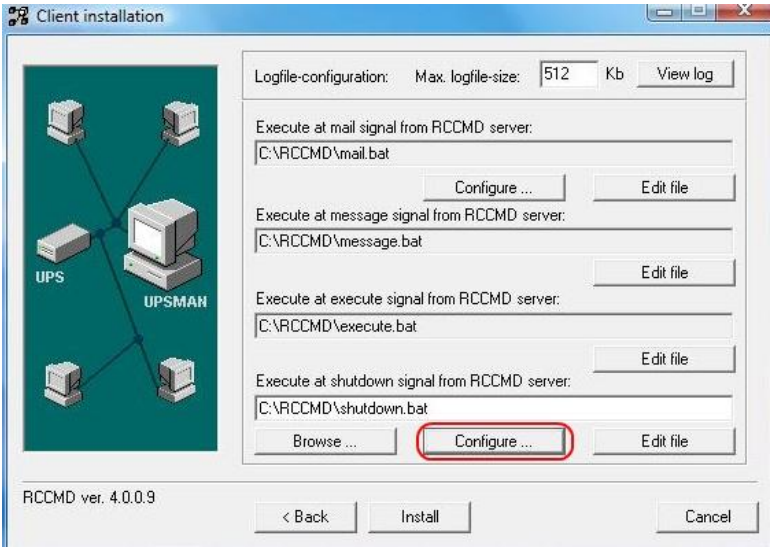


Figure 33 RCCMD Client Shutdown Configuration

Tag the “RCCMD shutdown relay” into the “Available Commands” window and click the “>” button, to add this function into the “Current Sequence”.

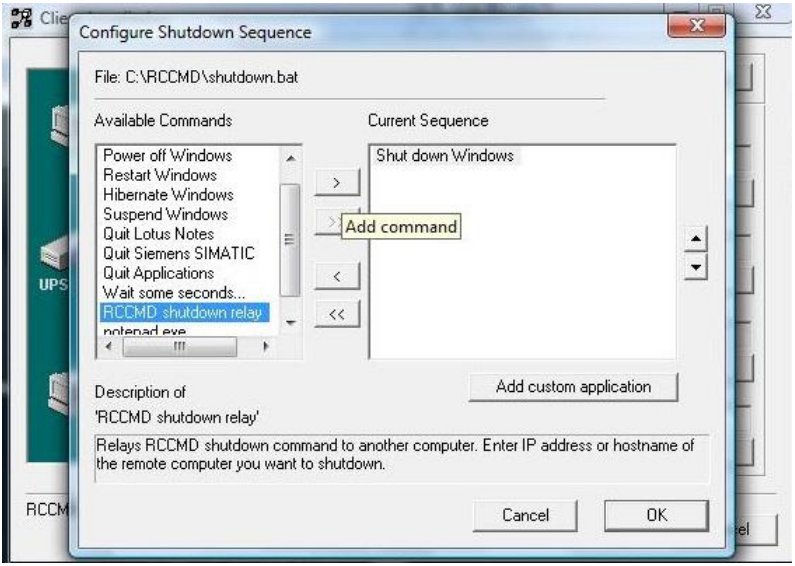


Figure 34 RCCMD Shutdown Relay

The following panel will appear, in which you can enter the desired IP address range.

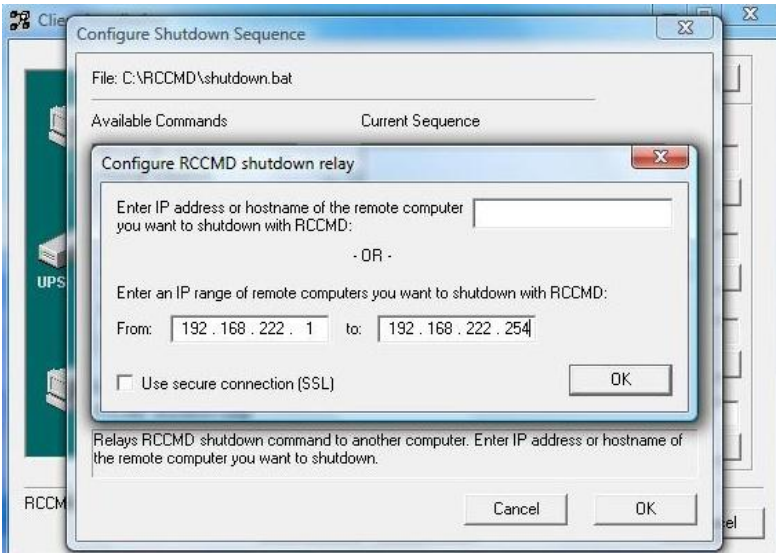

Configure Shutdown Sequence
File: C:\RCCMD\shutdown.bat
Available Commands
Current Sequence
Configure RCCMD shutdown relay
Enter IP address or hostname of the remote computer you want to shutdown with RCCMD:
- OR -
Enter an IP range of remote computers you want to shutdown with RCCMD:
From: 192 . 168 . 222 . 1
to: 192 . 168 . 222 . 254
Use secure connection (SSL)
OK
Relays RCCMD shutdown command to another computer. Enter IP address or hostname of the remote computer you want to shutdown.
Cancel
OK

Figure 35 RCCMD Configuration IP Address Range

Additionally you can enable the SSL function (see also chapter 3.8).

If you want to remove single IP addresses, mark the line with its desired IP address and click the “<” button.

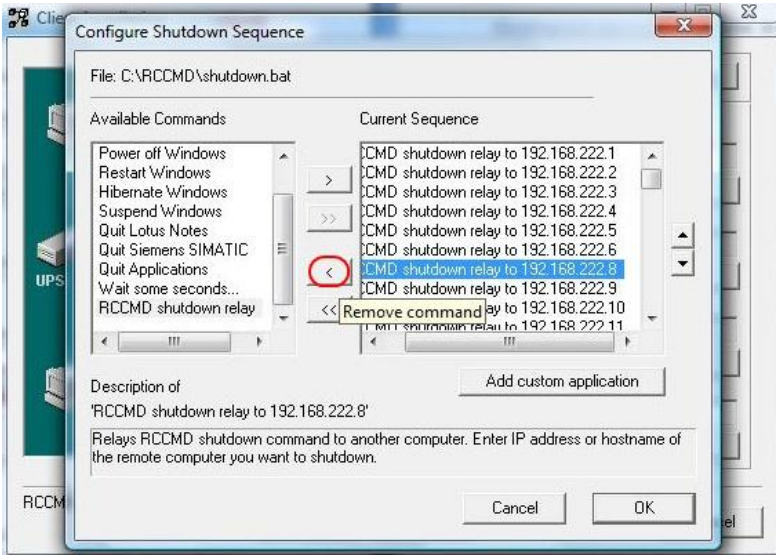


Figure 36 RCCMD Shutdown Relay Removal

3.6 RCCMD on Windows 95/98

RCCMD for Windows 95/98 functions similar to RCCMD on Windows NT. The only difference is the program name, which changes to RCCMD95.EXE. Please also refer to the RCCMD Windows section of this manual.

Attention: **For Windows 95/98 users we do recommend the installation of the TCP/IP protocol first and then run the configuration program making use of the RCCMD WIZARD.**

Attention: **In case Winpop.exe is used on Windows 95/98, RCCMD can not be started on port 6003 otherwise the computer will hang-up. Please change the sender and receiver call up accordingly.**

Experienced users may use the registry editor and enter all changes manually. Unexperiecend users should use the RCCMD wizard.

Registry settings: Please check the following: In order to start the RCCMD process in ”Listen” mode, the RCCMD parameter have to be entered in the registration database. Please enter:

regedit.exe rccmd95.reg or simply start rc_init.bat

The parameters are now located under the registration-key

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\RCCMD95\Parameters

Start *regedit.exe* again if you want to reconfigure RCCMD.

If you are unfamiliar with the registration editor of Windows 95 you can also modify the file *rccmd95.reg* and execute the command *regedit.exe rccmd95.reg* again.

Parameters:

Port: Special TCP-Port that receives the RCCMD signal.

Addr1... 10: TCP/IP address of the computer that accepts the RCCMD-signal.

ExecutePrg: Command that is to be executed when receiving the RCCMD-signal.

To start RCCMD execute the command:

rccmd95

Or start the program using the Windows 95/98-launch bar.

To start RCCMD in sending-mode (*send*) enter the following line in your shutdown-job:

RCCMD95 -s -a <address> [-p 6003]

For <*address*> enter the TCP-address of the machine to which you want to send the RCCMD-signal.

Optional parameters:

-p <port> TCP-Port on which the RCCMD-signal will be send

The option –a can be used several times, if a shutdown on more remote computers in the network should be executed.

Do not use the CD License key more than once. (Copyright regulations page 1). If more RCCMD modules need to be installed for the shutdown, additional CD license key must be purchased. Additional license keys are available from your UPS dealer, whereas the CD can be used again for the actual installation.

3.7 RCCMD for Windows NT/2000/XP/2003/2008

The RCCMD (remote console command) is a program that allows the execution of programs on remote computers. This tool is part of all UPSMAN supported operating systems with the exception of Windows 3.x.. With this tool it is possible to connect different operating systems. Is the UPS-Management Software installed on a Windows NT/2000/XP computer and should a remote shutdown be executed on a computer with a different operating system in a heterogeneous network, the RCCMD tool is necessary.

The RCCMD tool works in two different modes. The module works like a normal program start, as "Send Mode" in order to send RCCMD commands –s –a to other computers. In the so-called ”Listen” Mode, installed as a NT/2000/XP service, the program (as background process) waits for a command from ”Send Mode”, of the RCCMD module. In ”Listen Mode” the RCCMD module waits for the ”ping” signal. After reception of this signal the module executes a batch file or program.

Attention: **For first time users we do recommend the use of the RCCMD Wizard, which makes the configuration easier. Please start the RCCMD Wizard from your program group.**

Attention: **Please do not use the wizard and manual settings at the same time.**

Eventually, the RCCMD service must be allocated with special system privileges if certain commands and programs like messaging using “net send”, shutting down databases and the like are to be executed. The RCCMD start-up parameters in the control panel must be set to the administrator /superuser account (enter password twice) together with the correct password. If you are not allowed to use the administrator account you have to create an account, which has all the rights to shutdown this NT/2000 computer. Change to

the control panel and mark the RCCMD in the list, change the start-up parameters to ”this account” and enter the any administrative account.

Now the RCCMD has been installed and configured to execute C:\ups\shutdown.bat.

3.8 RCCMD with SSL for Windows

The Secure Sockets Layer (SSL) protocol is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks.

Use your Web-browser to navigate to the address of your UPS Web-Manager. Click the “Network & Security” configuration button and enable the SSL network feature.

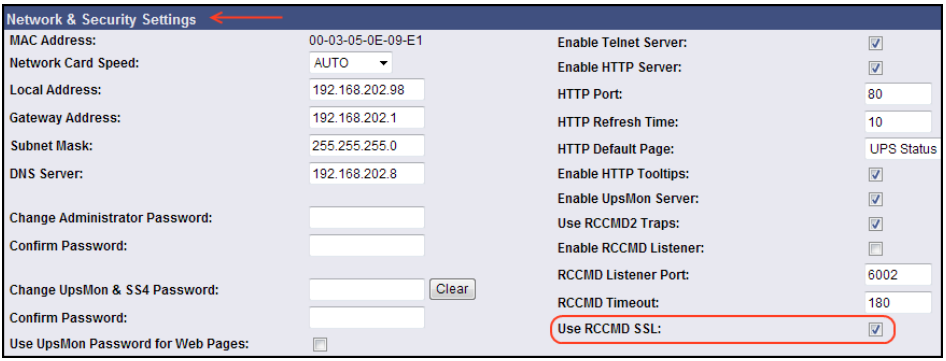


Figure 37 RCCMD SSL Settings

The SSL network feature requires correct time settings, so it is required to configure a timeserver. Click the „Timeserver“ configuration button and enter the address of at least one timeserver.

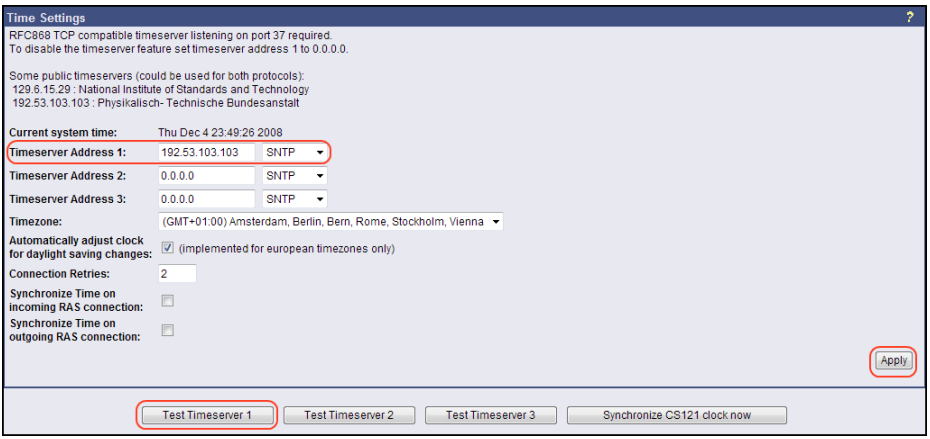


Figure 38 Timeserver Settings

Click the „Save Configuration“ button and the „Save, Exit & Reboot“ button to confirm your settings.

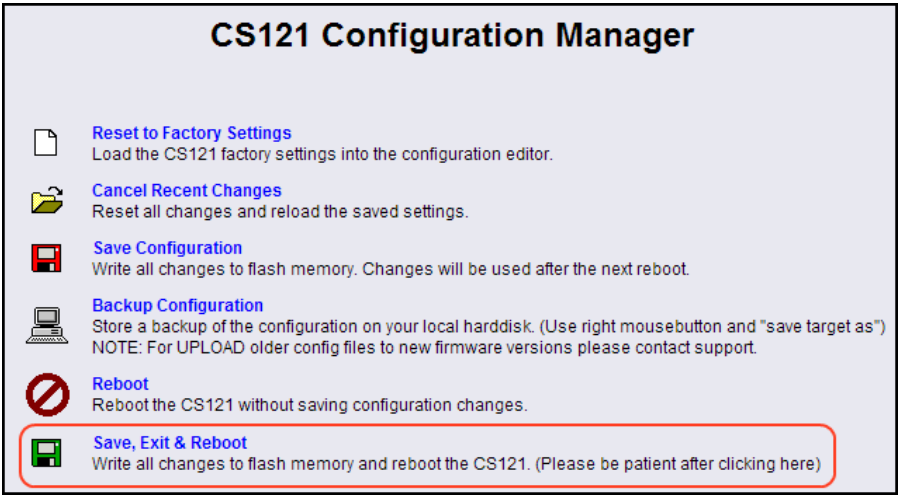

CS121 Configuration Manager
Reset to Factory Settings
Load the CS121 factory settings into the configuration editor.
Cancel Recent Changes
Reset all changes and reload the saved settings.
Save Configuration
Write all changes to flash memory. Changes will be used after the next reboot.
Backup Configuration
Store a backup of the configuration on your local harddisk. (Use right mousebutton and "save target as")
NOTE: For UPLOAD older config files to new firmware versions please contact support.
Reboot
Reboot the CS121 without saving configuration changes.
Save, Exit & Reboot
Write all changes to flash memory and reboot the CS121. (Please be patient after clicking here)

Figure 39 Settings Confirmation

Start the RCCMD Wizard installation again and enable the SSL network feature.

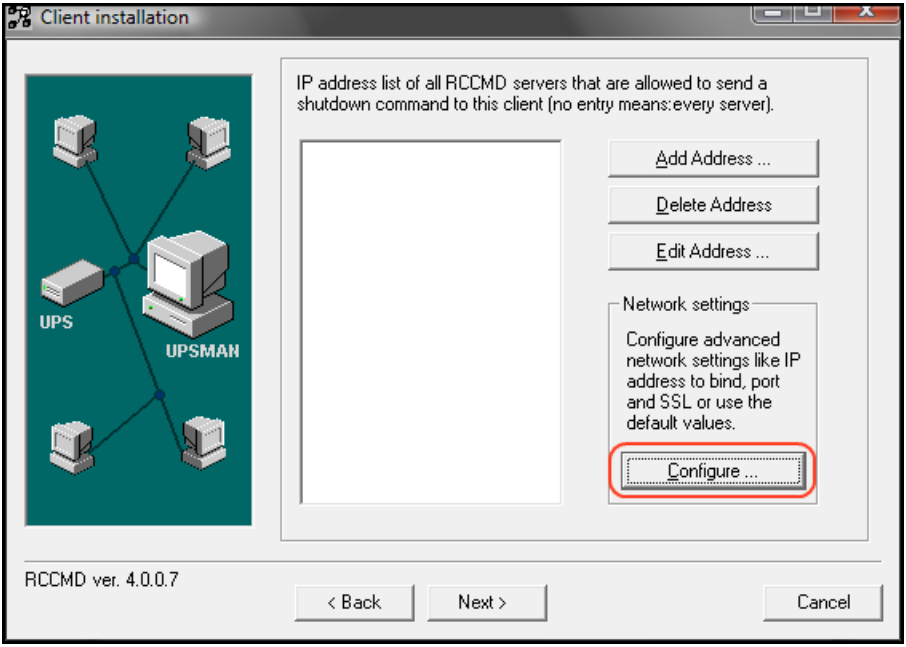

Client installation
UPS
UPSMAN
IP address list of all RCCMD servers that are allowed to send a shutdown command to this client (no entry means:every server).
Add Address ...
Delete Address
Edit Address ...
Network settings
Configure advanced network settings like IP address to bind, port and SSL or use the default values.
Configure ...
RCCMD ver. 4.0.0.7
< Back
Next >
Cancel

Figure 40 SSL Configuration

Figure 41 Advanced Network Settings

Alternative configuration with an ASCII editor

You can set the desired configuration with an ASCII editor into the configuration data „rccmd.cfg“ manually.

```
# RCCMD Configuration (v2-default)
#
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
#
ListenAddress=0.0.0.0
#
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
#
ListenPort=6003
#
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
```

```
# Default: true

#

ListenUDP=true

#

# Access Control List

# A list of valid sender addresses, only its members can connect
to us.

# Seperate IP addresses with a space, e.g.: "192.168.0.1
192.168.0.2".

# Default: <empty> (Everyone is allowed to connect to us)

#

AllowedAddresses=

#

# SSL: Use SSL

# Enables (true) or disables (false) SSL Connections

# Default: false

#

SSL=false

#

# SSL: Reject expired certificates

# Permits (false) or denies (true) connections with expired
cert's.

# Default: false

#

SSLRejectExpiredCert=false
```

The SSL configuration occurs via the following entries:

```
SSL=true

SSLRejectExpiredCert=false
```

During the installation you can merge the grafical configuration and create a narrated „rccmd.cfg“ at the same time, if you answer the following question:

```
This is NOT an ITANIUM (IA-64) system [Y/n]?:
```

with „n“.

3.8.1 RCCMD with own SSL certificates

In this chapter we will describe, how to use an own SSL certificate with RCCMD, e. g. OpenSSL (http://www.openssl.org/related/binaries.html):

Be your own CA

Using OpenSSL it is quite simple to become your own CA. Just run:

```
CA.pl –newca
```

Done! Just ensure, that you select a useful CN (common name)!

Create your RCCMD certificate

You need to create your certificate for RCCMD now. As it will use it for verification, it should contain the same useful common name (CN), that you selected for the CA. The private key must not be encrypted to let the RCCMD Client (service) start without trouble. Therefore we use the “–nodes” option and the “-newreq” command:

```
CA.pl –newreq -nodes
```

Sign with your CA:

```
CA.pl –sign
```

Now create an empty file named “rccmd.pem“ and copy the cert information of *newcert.pem* (rccmd certificate), *newkey.pem* (private key) and *cacert.pem* (CA) into it. Please note, that the exact copying is required to use it without trouble!

Use your own RCCMD certificate

Do the following steps at the RCCMD Client and every sender (e. g. UPS Web Manager):

- Backup the existing “rccmd.pem”
- Replace the existing “rccmd.pem” with your own
- Restart the RCCMD Client
- Restart the RCCMD Sender

3.3.5 Testing the RCCMD connection

Finally test your configuration if all RCCMDs are present and working. For this you may use the RCCMD in the Debug mode Syntax RCCMD –debug –s/l –a), so that you have screen output. ”PING” every remote computer with the command ”ping [hostname] [IP

address]". If the PING works fine, you can now start to test the RCCMD connection with the debug mode. If everything works fine, you will see that a connection is established and closed again. This means that the remote RCCMD received your signal and will execute the shutdown script on the remote side.

ATTENTION! This test will execute the shutdown script! If you want to avoid the shutdown, please remove the shutdowncommand from the RCCMD client shutdown.bat/sh file!

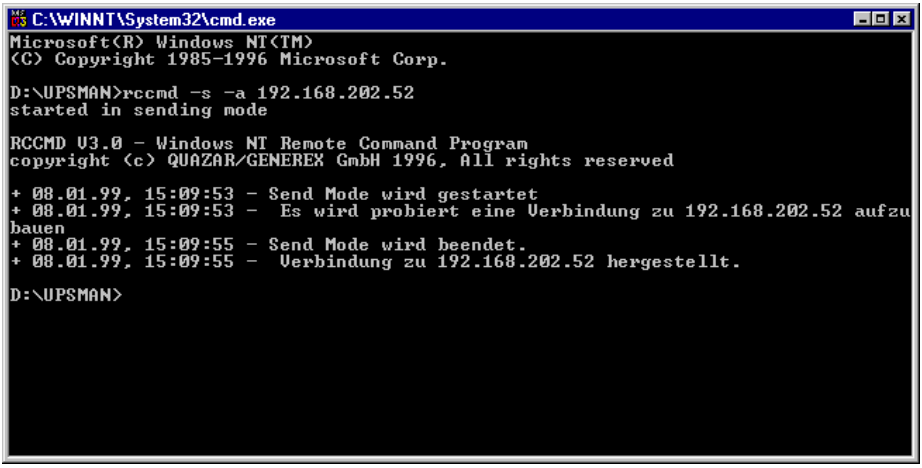

C:\WINNT\System32\cmd.exe
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.
D:\UPSMAN>rccmd -s -a 192.168.202.52
started in sending mode
RCCMD V3.0 - Windows NT Remote Command Program
copyright (c) QUAZAR/GENEREX GmbH 1996, All rights reserved
+ 08.01.99, 15:09:53 - Send Mode wird gestartet
+ 08.01.99, 15:09:53 - Es wird probiert eine Verbindung zu 192.168.202.52 aufzu
bauen
+ 08.01.99, 15:09:55 - Send Mode wird beendet.
+ 08.01.99, 15:09:55 - Verbindung zu 192.168.202.52 hergestellt.
D:\UPSMAN>

Figure 42 RCCMD Console Test

3.9 Testing the RCCMD 2 connection

In order to see under RCCMD 2 if the UPSMAN processes on the remote client are still active, the following syntax can be entered via command line:

rccmd –sc –ac <IP address>

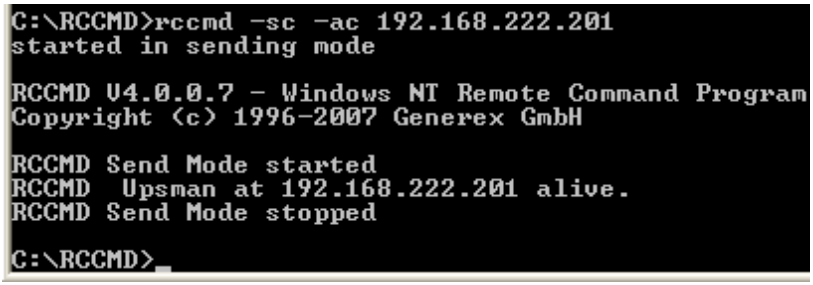

C:\RCCMD>rccmd -sc -ac 192.168.222.201
started in sending mode
RCCMD V4.0.0.7 - Windows NT Remote Command Program
Copyright (c) 1996-2007 Generex GmbH
RCCMD Send Mode started
RCCMD Upsman at 192.168.222.201 alive.
RCCMD Send Mode stopped
C:\RCCMD>

Figure 43 RCCMD Alive Check via Command Line

If the UPSMAN is active, the message "UPSMAN <IP address> alive". There is no message if the UPSMAN is inactive.

Testing the RCCMD 2 connection via the “Alive Check” option of the RCCMD Wizard: If you want to use the UPSMAN alive checking (recommended), check the “Enable connection check” box. Alive check is a signal, send out to the UPSMAN or CS121 on port 5769 to check if the UPSMAN has still UPS data – or not.

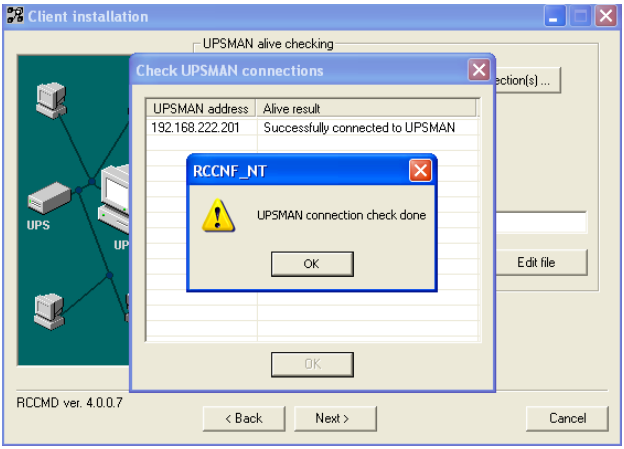


Figure 44 UPSMAN Alive Check Window

Use this command to get help: `C:\RCCMD>rccmd -?`

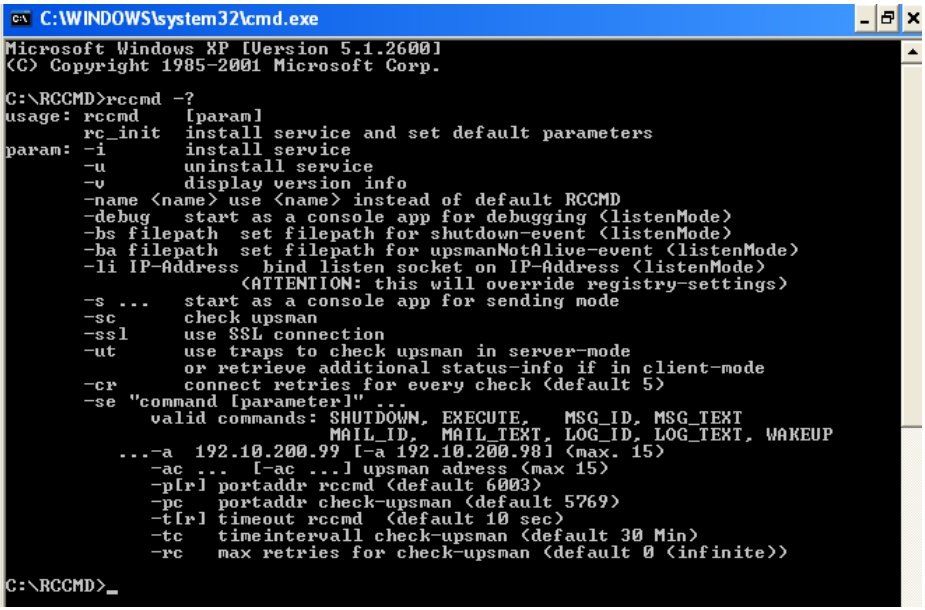

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\RCCMD>rccmd -?
usage: rccmd [param]
rc_init install service and set default parameters
param: -i install service
-u uninstall service
-v display version info
-name <name> use <name> instead of default RCCMD
-debug start as a console app for debugging (listenMode)
-bs filepath set filepath for shutdown-event (listenMode)
-ba filepath set filepath for upsmanNotAlive-event (listenMode)
-li IP-Address bind listen socket on IP-Address (listenMode)
(ATTENTION: this will override registry-settings)
-s ... start as a console app for sending mode
-sc check upsman
-ssl use SSL connection
-ut use traps to check upsman in server-mode
or retrieve additional status-info if in client-mode
-cr connect retries for every check (default 5)
-se "command [parameter]" ...
valid commands: SHUTDOWN, EXECUTE, MSG_ID, MSG_TEXT
MAIL_ID, MAIL_TEXT, LOG_ID, LOG_TEXT, WAKEUP
...-a 192.10.200.99 [-a 192.10.200.98] (max. 15)
-ac ... [-ac ...] upsman adress (max 15)
-p[r] portaddr rccmd (default 6003)
-pc portaddr check-upsman (default 5769)
-t[r] timeout rccmd (default 10 sec)
-tc timeintervall check-upsman (default 30 Min)
-rc max retries for check-upsman (default 0 (infinite))
C:\RCCMD>

Figure 45 RCCMD Console -?

3.10 RCCMD on NovellNetWare

The following text is presented when entering RCCMD with the help parameter “?” inside a NovellNetWare console:

```
Possible parameters:

 -l
     listen. waits for a command from RCCMD sender

 -s
     sends a ping to a listening program

 -se <command> <param>
     sends a command to a listening program

 -p  <port>
     Portadress (Defaultadress = 6003)

 -a  <ipaddress>
     Address in IP Format. Ex. -a 192.10.20.30 (max.
10)

 -t  <timeout>
     Time in Seconds (Defaulttimeout = MAX_TIMEOUT)

 -?
     this help

Supported Commands (for use with -se argument):

 SHUTDOWN
          This will call the configured shutdown-
batchfile (default: shutdown.bat)

 EXECUTE
          This will call the execute.bat file

 MSG_TEXT
          This will call the message.bat file
<text, unrestricted word count>

 MSG_ID <ID>
          This will call the message.bat file
<message parameters, seperated by blanks>

 LOG_TEXT
```

```
          This will write to configured log-file
(default: rccmd.log) <text, unrestricted word count>

 LOG_ID <ID>
          This will write to configured log-file
(default: rccmd.log) <message parameters, seperated
by blanks>

Examples:

 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
-t 10
 load rccmd.nlm -se "SHUTDOWN" -a 192.10.200.52

 load rccmd.nlm -se "EXECUTE" -a 192.10.200.52
 load rccmd.nlm -se "MSG_TEXT this is a message" -a
192.10.200.52
 load rccmd.nlm -l
 load rccmd.nlm -l -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -l -a 192.10.200.52

If you have added a search path i.e.: "search add
sys:rccmd",
otherwise you have to use the absolute path.

 load sys:rccmd\rccmd.nlm -l
```

To start RCCMD in receiving-mode (*listen*) enter the following line:

load <path> RCCMD -l [-a 192.200.100.10] [-p 6003] load <path> shutcmd.nlm –f

Optional parameters:

-a <address> TCP/IP address of the master computer(s), which sends the RCCMD-signal.

-p <port> (optional) TCP-Port address, on which the master computer is sending

To start RCCMD in sending-mode (*send*) enter the following line in your shutdown-job:

load RCCMD -s -a <address> [-p 6003]

For *<address>* enter the TCP-address of the machine to which you want to send the RCCMD-signal. (Workstations in "listening" mode, with an active RCCMD with parameter -l)

Optional parameters:

-p <port> TCP-Port, which the RCCMD-signal is using.

The option -a can be used multiple times, if a shutdown on remote network servers should be initiated.

Example: (Example path <path> = sys:\ups\upsman\rccmd.nlm)

load <path> RCCMD.NLM –s –a 192.168.210.3 -a 192.168.210.4 -a 192.168.210.10

...etc.until ”end of line”

unload RCCMD

load <path> RCCMD.NLM –s –a 192.168.210.8...etc.

unload RCCMD

Do not use the CD License key more than once. If more RCCMD modules need to be installed for the shutdown, additional CD license keys must be purchased. Additional license keys are available from your UPS dealer, whereas the CD can be used again for the actual installation.

rccmd.nlm

Modul for the multiserver shutdown in IP-networks.

The rccmd.nlm contains different command line parameters, which are either for the ”send” or ”listen” modul of the RCCMD modul.

rccmd -? Help

rccmd -s Sending off a ”ping” signal to a waiting program

rccmd -l Waiting for a ”ping” signal. A command can be executed after the reception of the ”ping” signal.

rccmd –p Setting the port address (default = 6003).

rccmd –a Address in IP format e.g. 192.168.202.1

rccmd –t Time in seconds until a connection will be established. (default timeout = 10)

Example:

load sys:ups\rccmd.nlm -s -a 192.168.202.1 [-a 192.168.202.1]

load sys:ups\rccmd.nlm -s -a 192.168.202.1 -t 10

load sys:ups\rccmd.nlm -l -a 192.168.202.1 shutcmd.nlm [/para]

rccmdipx.nlm

This is a modul for just IPX networks. This modul sends a shutdown command (or any other console command) directly to every IPX server name. Please start RCCMDIPX on all Novell consols. The modul needs to be loaded on both servers.

This modul has to loaded on both servers first

(1. Rename RCCMDIPX to RCCMS.NLM 2. Load RCCMD The following syntax is valid:

rccmd <server name> <console command>

Whereas <server name> is a valid server in a network enviroment and <console command> a valid NetWare command is.

Example:

1. load sys:ups\rccmdipx (or load RCCMD if RCCMDIPX.NLM is renamed to RCCMD.NLM)

2. rccmd gnw1 forcedown

or 1. load sys:ups\rccmdipx

2. rccmd gnw1 sys:ups\down.ncf

Instead of the down command for older *clib.nlm* files, the *forcedown* command maybe used.

Multiple-start RCCMD on Novell

The multiple start RCCMD on Novell is relatively easy to manage. Several RCCMD clients may be started with the following command line:

load rccmd.nlm -l -a load down.ncf

whereas the syntax goes as follows:

LOADING RCCMD.NLM -L(LISTENER) -A(IP adress of UPSMAN/CS121/RCCMD SENDER) COMMAND (COMMAND TO BE EXECUTED)

Example:

LOAD RCCMD.NLM -L -A 192.168.10.2 LOAD DOWN.NCF

In this scenario the “down.ncf“ file is executed, which leads to an immediate shutdown of the client computer, if the RCCMD call from the RCCMD server (sender) is received. Other . ncf or .nlm (executables) files may be executed too.

A group of 8 .ncf example files can be found in the UPSMAN installation directory. Please note that these example files ma have to be adjusted by user/administrator according to the configuration of the system.

4. RCCMD on UNIX (with graphical interface)

The RCCMD (remote console command) is a program that allows the execution of programs on remote computers. This tool is part of all UPSMAN supported operating systems as well as all GENEREX CS121 SNMP Manager, BACS Webmanager or RCCMD licensed SNMP Manager of other manufacturers (Rittal CMC, General Electric SNMP, Chloride Masterguard). With this tool it is possible to connect different operating systems. E.g. is the UPS-Management Software installed on a Unix computer and should a remote shutdown be executed on a computer with a different operating system in heterogene network, the RCCMD tool is necessary.

The RCCMD tool is based on the TCP/IP protocol. During the installation, the TCP/IP protocol should be installed in the first place.

The RCCMD tool works in two different modes. In the so called ”Listen” mode, the program (as UNIX daemon in a background process) waits for a command from the ”Send” mode of the RCCMD modul.

INSTALLATION

It is required to install RCCMD as user root out of a rootshell or a graphical terminal. Extract the file **rccmd.tar**, copy it to a temporary folder and start the program **rccmd.bin**. The following graphical installation will start:

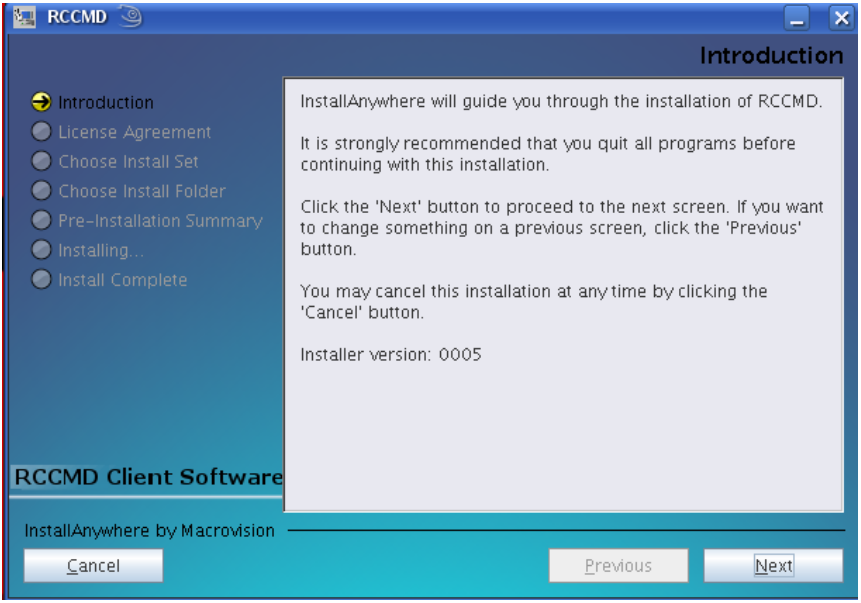

RCCMD
Introduction
Introduction
License Agreement
Choose Install Set
Choose Install Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere will guide you through the installation of RCCMD.
It is strongly recommended that you quit all programs before continuing with this installation.
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.
You may cancel this installation at any time by clicking the 'Cancel' button.
Installer version: 0005
RCCMD Client Software
InstallAnywhere by Macrovision
Cancel
Previous
Next

Figure 46 Installation – Introduction

Enter your license key:

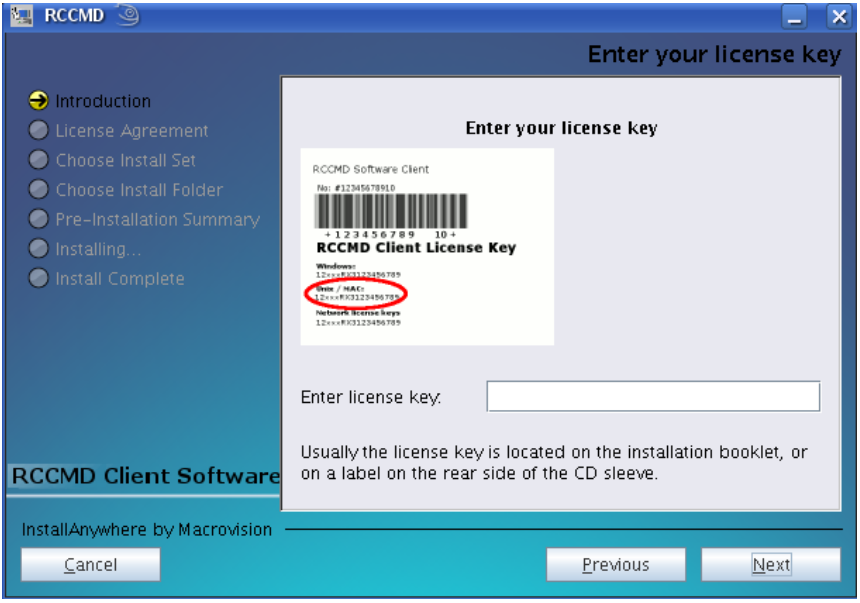


Figure 47 Installation – License Key

Choose your desired installation path.

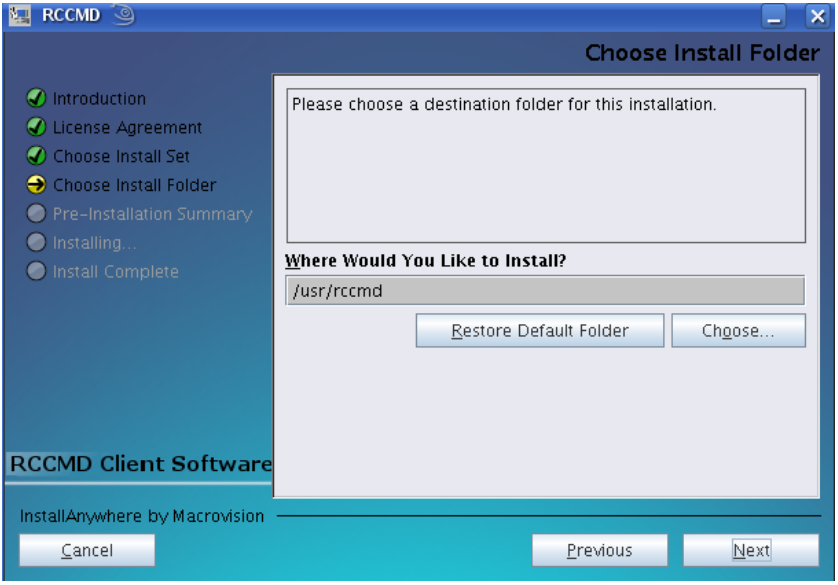


Figure 48 Installation – Choose Install Folder

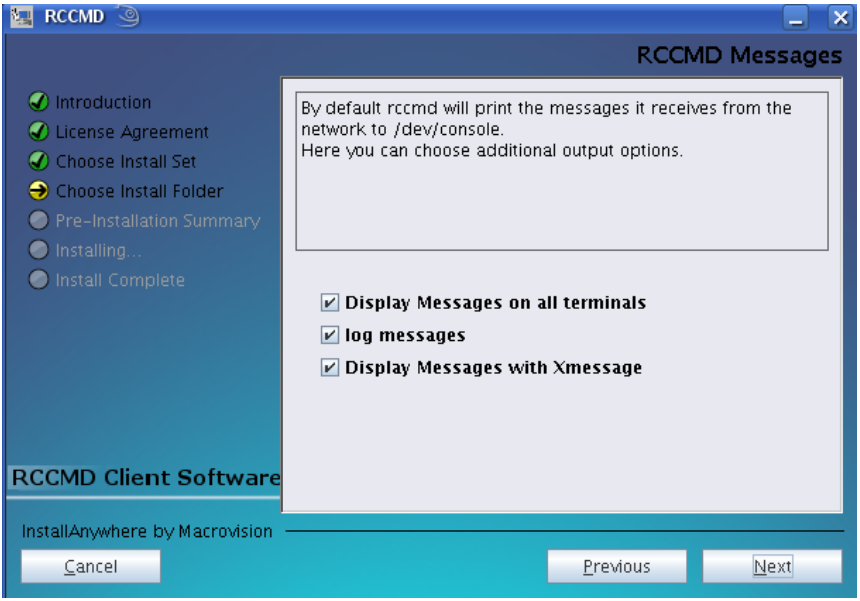


Figure 49 Installation – RCCMD Messages

In the next menu you see an overview of your installation and you may now press “Install” to begin.

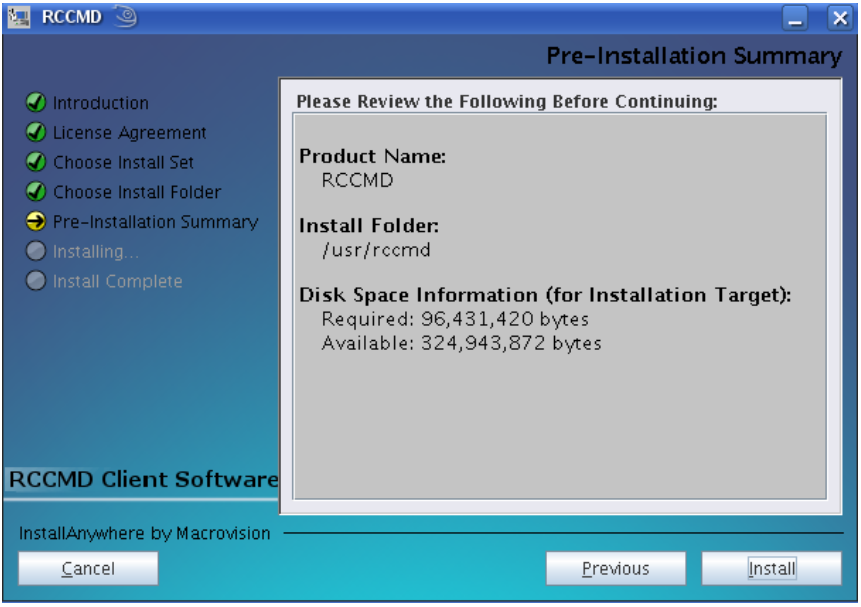


Figure 50 Installation – Pre-Installation Summary

Add the IP address of the RCCMD server, which is allowed to send a shutdown to this client.

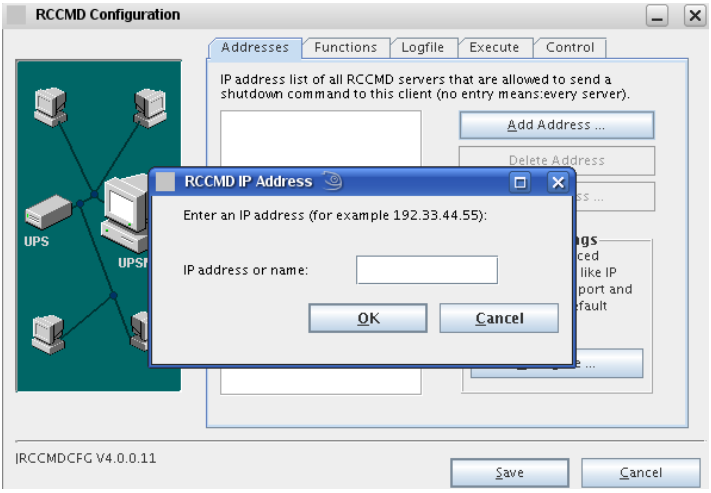


Figure 51 Configuration – RCMD Sender IP Address

Attention:

If you do not enter an address, then every server has the permission to send a shutdown command. If more than one CS121 or rather UPSMAN is existent, thus a redundancy situation, you need to enter more than one address as authorized sender.

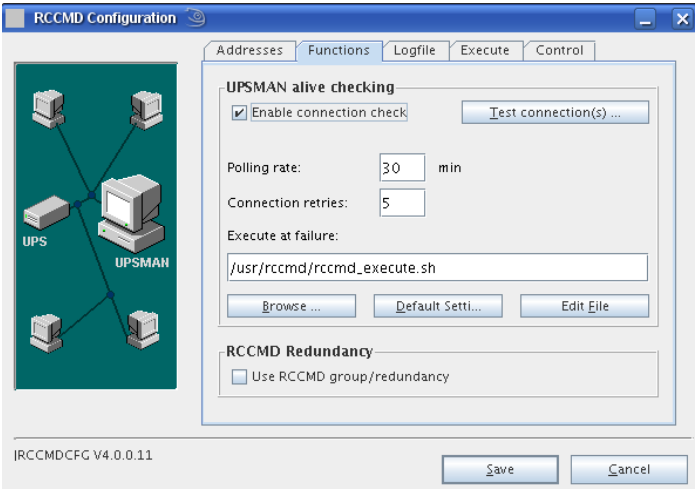


Figure 52 Configuration – RCMD Functions

If you want to use the UPSMAN alive checking (recommended), check the “Enable connection check” box. Alive check is a signal, send out to the UPSMAN or CS121 on port 5769 to check if the UPSMAN has still UPS data – or not. If this fails, the scriptfile rccmd_execute.sh will be executed which causes a messagbox coming up. The polling rate (default 30 min.) defines the polling of the UPSMAN service, connect retries (default 5) means after 5 unsuccessful connection tries an alarm will be triggered.

The function “Use RCCMD Traps” enables UPSMAN/RCCMD/UNMS traps, which show the UPS status as a trap message. If activated it will display a local message when the UPS status of the UPSMAN/RCCMD server changes.

If you click the “Test connection(s)…” button, the UPSMAN alive checking of the entered IP addresses will start (port 5769 will be tested).

If you click the „Browse...“ button, you will get a selection of the default sh-files.

At UPS installation RCCMD offers redundancy management functionality as follows:

Every UPS must be equipped with a CS121 or UPSMAN software computer. When ticking the box “use RCCMD group/redundancy” – you are guided to a menue where you can choose which CS121 /UPSMAN are supplying this RCCMD client. E.g. if 4 CS121/UPSMAN are installed into 4 UPS – than each may send a shutdown signal to this RCCMD client.

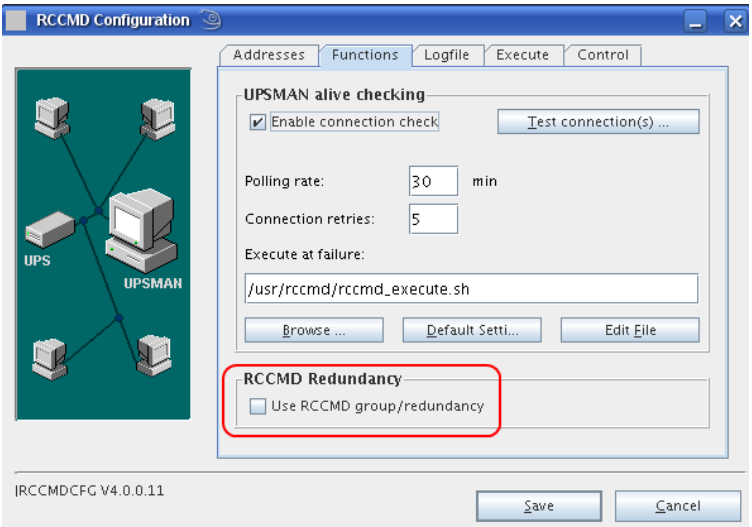


Figure 53 Configuration – RCMD Redundancy

The redundancy level defines how many shutdown signals are required to execute the shutdown.bat file. As long as this number is not exceeded, the RCCMD client will react on such a shutdown signal only with a messagebox “Execute command when redundancy suppresses a shutdown” box. This will show a message to inform the user that there has

been a shutdown signal from one of the UPS in the group, but since all other UPS are still reading OK – or did not yet send any shutdown, the shutdown is suppressed. 3 shutdown signals would create messages in the above example (redundancy level 3) only, just the 4th signal would initiate the shutdown.

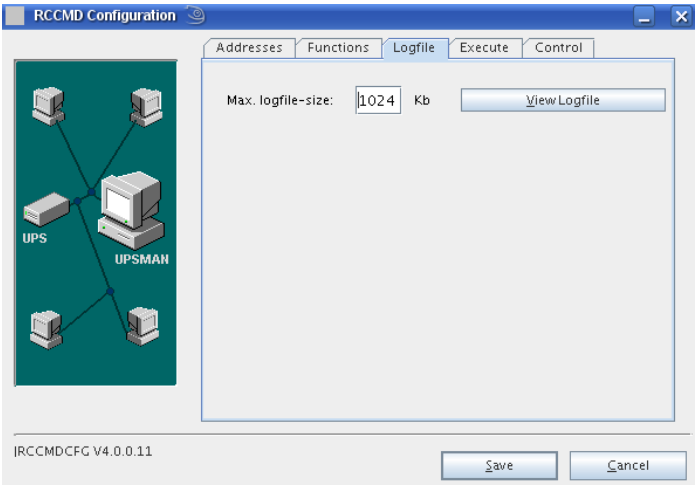


Figure 54 Configuration – RCMD Log File

You can configure the log file size and edit the executing sh-files.

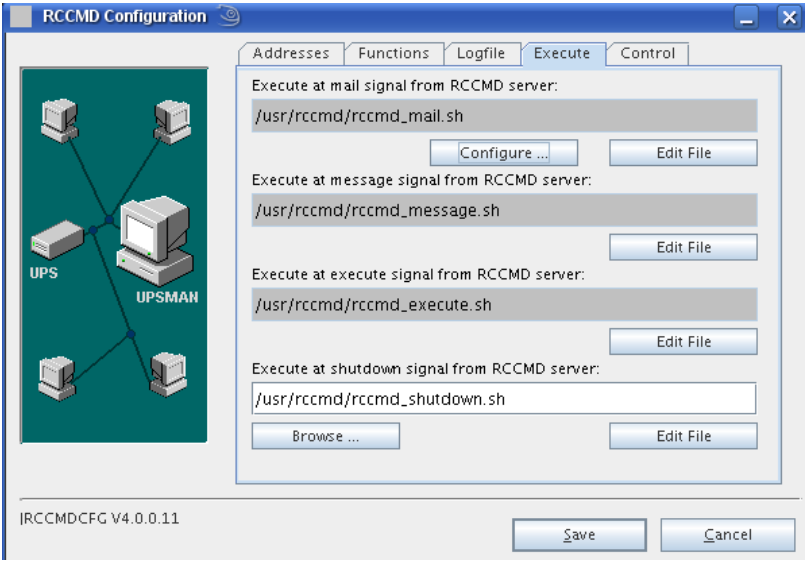


Figure 55 Configuration – RCMD Execute

Click the “Configure…” button to enter the E-Mail settings.

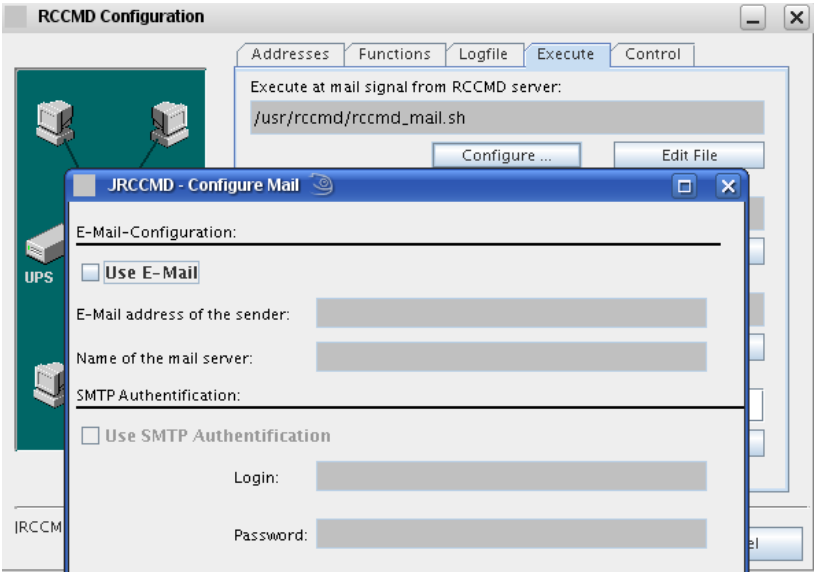


Figure 56 Configuration – RCMD E-Mail Configuration

Click « Control » to get to the following functions:

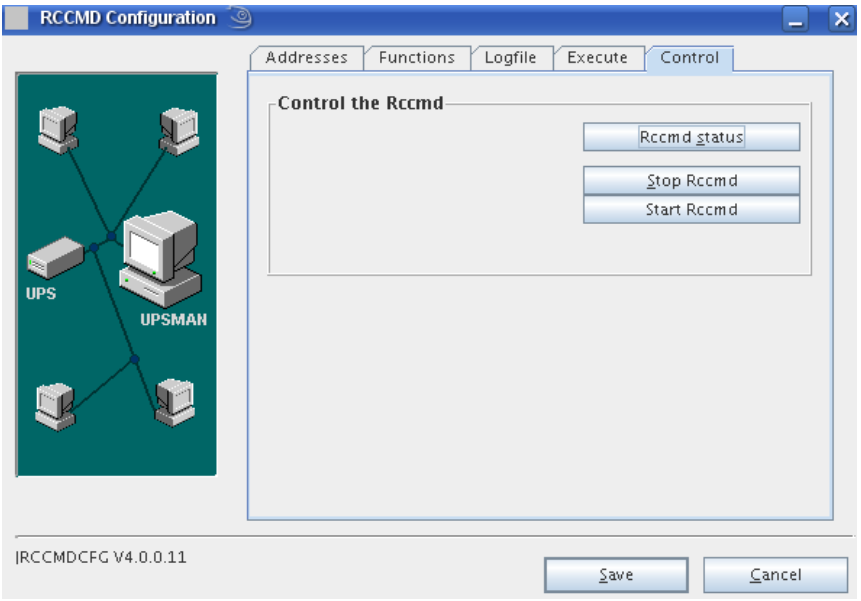


Figure 57 Configuration – RCMD Control

4.1 Silent Installation of the RCCMD Installation

The RCCMD Software provides a silent installation, but it is required to enter some settings into the “installer.properties” file.

```
## This file provides Values to alter the behaviour of the installer.
## You can preset Values for some internal Variables.
## For the installer to find and use this file it is necessary to either rename
##  this file or pass a parameter to the installer when calling it.
##
## If this file is called 'installer.properties' or has the same name as the
##  installer, e.g. 'install_RCCMD.properties' then the installer should
##  automatically use this file.
##
## To call the installer with a parameter providing a properties file, the
##  installer need the parameter '-f' in this case the command line call looks
##  somewhat like this: "install_RCCMD.exe -f silent-installer.properties".
##
## To set the installer User Interface without providing the variable in the
##  properties file, the parameter '-i' can be used.
##  E.g. "install_RCCMD.exe -i silent"
##  The interface options are "silent,gui,console" the gui option is default.

## This will set the User Interface of the installer
#INSTALLER_UI=silent

## This presets the Licensekey. This value is necessary for a silent
##  installation, because there is no other way to pass this information to
##  the installer.
#GXLICENSEKEY=

## The Dialogbutton variable contains the answer to the pop-up questions whether
##  the RCCMD should be started at system boot and wether it should be started now.
##  the value '0' resembles the answer 'Yes' the value '1' (default) corresponds
##  to 'no'.
#CHOSEN_DIALOG_BUTTON=0

## Select the language for the installed version of RCCMD by setting the
##  INST_LANG variable to the desired country-code
##  (e.g.: el,en,es,de,fr,he,it,ja,ko,pt,ru,tr,zh_cn).
#INST_LANG=en
```

Figure 58 Content of the “installer.properties”

It is required to remove the hash mark prior of the variable `INSTALLER_UI=silent`. In addition the setting of the license key is required behind the variable `GXLICENSEKEY=`.

If you want to activate the console installation, it is required to remove the hash mark prior of the variable `INSTALLER_UI=console` and to set the word console instead of silent.

4.2 Console Installation of the RCCMD Installation

A console installation is required, if your target system possesses no grafical interface for the execution of the “installRCCMD.bin”. This console installation works interactive and will display the questions, which are containing into the “installer.properties” file.

Note: **This concerns the installation only. The configuration will be performed via editor into the „rccmd.cfg“ file.**

For the activation of the console installation, it is required to remove the hash mark prior of the variable `INSTALLER_UI=` and to enter `console`. This is the interactive RCCMD installation onto the console. Execute as `root` the “installRCCMD.bin” file.

Configuration

It is required to perform the configuration via editor. The configuration file is the “rccmd.cfg” and is located into the /usr/rccmd folder (default). The file contains the description of the single configuration parameters. Please take a look into the following example of the “rccmd.cfg” file:

```
#######################################
# RCCMD Configuration
#######################################
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
ListenAddress=0.0.0.0
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
ListenPort=6003
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
ListenUDP=true
# Access Control List
# A list of valid sender addresses, only its members can connect to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
AllowedAddresses=
# Alive Check
# Enable Alive Check
```

Defines if we should perform UPSMan alive checking.

Default: false

AliveEnabled=false

Alive Check Rate

Defines the interval of UPSMan alive checking, in seconds.

Default: 1800

AliveInterval=1800

Alive Retry Rate

Defines the number of UPSMan alive checking retries, in case of problems.

Default: 0

AliveRetries=5

Alive Check Group Members List

A list of UPS device addresses that should be checked periodically.

Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

Default: <empty> (No alive checking)

AliveAddresses=

Alive Program

Full path to script that is executed when an alive check fails.

Default: rccmd_notalive.sh

AliveProg=

Redundacy Mode

Enable Redundancy

Defines if we should operate in redundancy mode.

Requires an enabled <Alive Check> configuration.

Default: false

RedundancyEnabled=false

Redundancy Group Members List

A list of redundancy group member addresses, must be also in <AliveAddresses>.

Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".

Default: <empty> (No redundancy available)

RedundancyAddresses=

Redundancy Level

Defines how many of the <RedundancyAddresses> are redundant.

Shutdown is executed when the number of shutdown requests exceeds this number.

Default: 0 (No redundancy available)

RedundancyLevel=0

Enable Redundancy Script

Defines if we should NOT execute a script when redundancy suppresses a shutdown.

Default: false.

RedundancyBatchSuppress=false

Redundancy Script

Full path to script that is executed when redundancy suppresses a shutdown.

Default: ShutdownSuppressed.sh

RedundancyBatchFile=

4.3 UNIX RCCMD Configuration With CURSES Library

Note: **This section does not apply to rccmd V1 for Unix, in addition it only applies to rccmd running in 'Listen' mode.**

Rccmd V2 running in 'Listen' mode may be configured using a configuration file. By default rccmd will look for a file named 'rccmd.cfg' in its startup directory (usually '/usr/ups'). This file may be generated using rccmd_conf. Rccmd_conf is a small curses-based utility which runs on the console or a terminal or a terminal-emulation under the X Window System (e.g. xterm).

Note: **The contents of 'rccmd.cfg' are vital to system security. It should be writeable only for the System User 'root'.**

Run rccmd_conf:

$ su -

Password:

cd /usr/ups

./rccmd_conf

if 'rccmd.cfg' does not exist (e.g. if you run rccmd_conf for the first time) the following notice will be displayed:

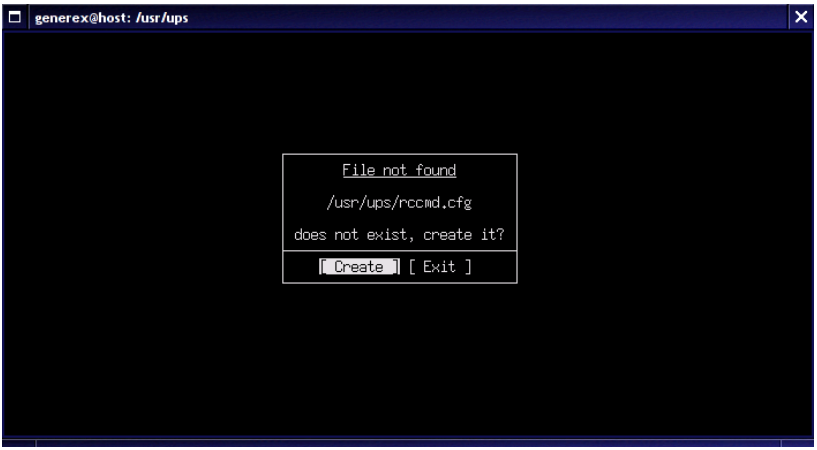


Figure 59 Making the Configuration File

To proceed hit the [Tab] key until the [Create] button it is highlighted and press [Enter], otherwise select [Exit].

If you created 'rccmd.cfg' or if the file existed already rccmd_conf will switch to its main configuration menu.

Figure 60 RCCMD Configuration Menu UNIX

To switch between the menu entries use the [Tab] key and/or the arrow keys [←], [→], [↑] and [↓]. To select an entry press [Enter].

It is not necessary to work from top to the bottom, you may configure the menu items in any order. In fact it is not necessary to configure anything at all, if you just select [save] 'rccmd.cfg' will be written with default values sufficient to run rccmd. To use all features of rccmd and/or improve security it is however strongly suggested to customize 'rccmd.cfg'.

Configure “Rccmd Network Options”

In this screen you may configure network related options of the rccmd listener. To switch between the option-fields and buttons use the [Tab] key.

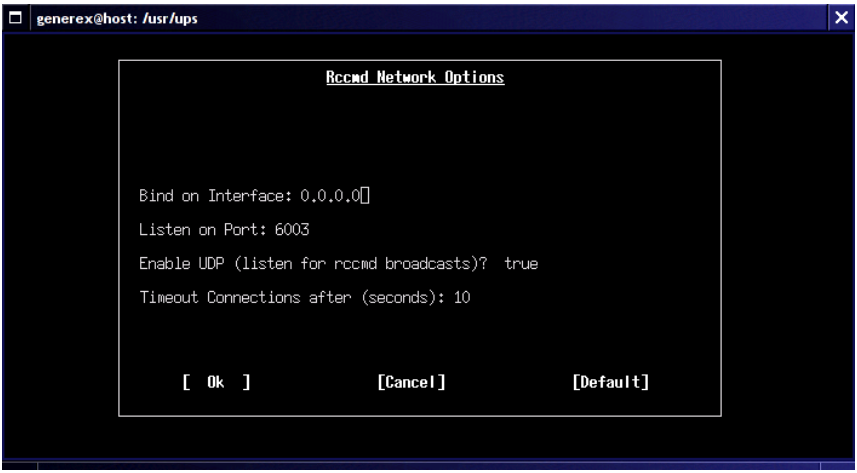


Figure 61 RCCMD UNIX Network Options

Bind on Interface:

This option tells rccmd on which network interface it binds its main tcp listen socket. You may enter any valid IP address your host can be reached.

The default value for this option is 0.0.0.0, this is a working value, it means 'listen on all possible interfaces of this host'. If your host has a dial up connection to the internet you may want to change the default, to ensure rccmd will not be connected from the internet. In this case you will enter the primary IP address of the host rccmd listener is running on.

Example:

	Your company runs a private network in the 192.168.1.0/24 address range. The host rccmd listener is running on is assigned the IP 192.168.1.9. You may enter 192.168.1.9 for “Bind on Interface”, to ensure only host from the private network can connect to rccmd.
Listen on Port:	This is the port rccmd will listen to. Allowed values range from 1 to 65535 (inclusive). The default is 6003. If you change the port of the rccmd listener you will also have to switch the port of the rccmd sender in order to enable a connection. It is normally not necessary to change this setting.
Enable UDP:	If this opion is enabled rccmd will open an UDP Listen Socket in addition to the TCP Socket. This allows the rccmd listener to receive rccmd broadcasts. Possible values are 'true' and 'false'. The default is “true”. To switch the value use the [↑] and [↓] keys.
Timeout:	Timeout for TCP connections. The default is 10 seconds. It is normally not necessary to change this setting.

To reset all values to their defaults select the [Default] button by hitting the [Tab] key, then press [Enter].

To leave the screen select either [Ok] or [Cancel] with the [Tab] key and press [Enter], [Ok] means accept all values as displayed on the screen, [Cancel] means discard all changes made to the screen.

Configure “Access Control List”

“Access Control List” contains a list of valid sender addresses. A valid sender address is the IP address of an rccmd sender that is allowed to connect to the rccmd listener. Initially the list is empty.

Note: **An empty Access Control List means everyone is allowed to connect.**

To switch between the entries in the list use the [↑] and [↓] keys, to switch between the buttons use the [Tab] key. To select an entry press [Enter].

Figure 62 RCCMD UNIX Add Sender

To add an IP address hit the [Tab] key until the [Add] button is highlighted, then press [Enter].

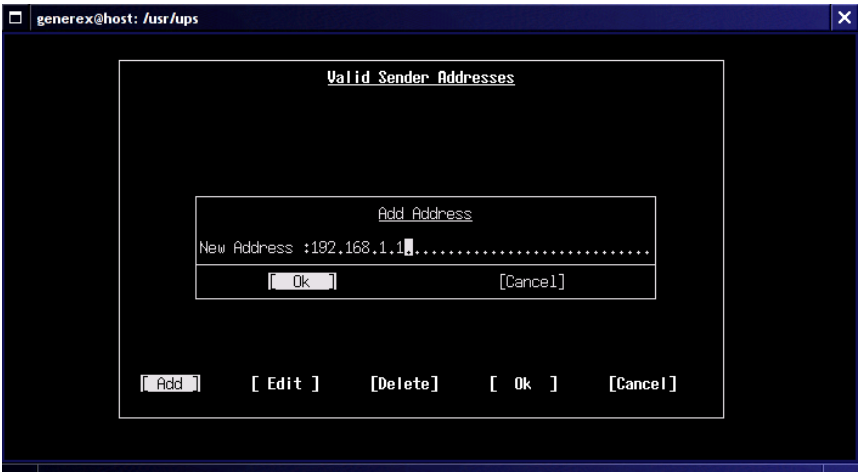


Figure 63 RCCMD UNIX Sender Example

Enter the IP address of the host you want to be able to connect, then press [Enter].

Figure 64 RCCMD UNIX Sender Overview

To edit an entry in the list select it by hitting the [↑] and [↓] keys until the entry is highlighted, then hit the [Tab] key until the [Edit] button is highlighted, then press [Enter].

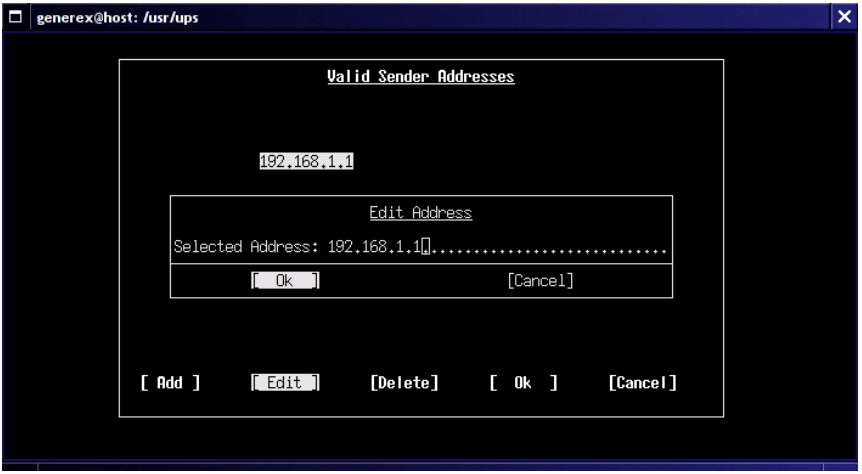


Figure 65 RCCMD UNIX Edit Sender

Edit the Address in the “Edit Address” Window. To keep your changes select the [Ok] button with the [Tab] key and press [Enter] otherwise select [Cancel].

To delete an entry in the list select it by hitting the [↑] and [↓] keys until the entry is highlighted, then hit the [Tab] key until the [Delete] button is highlighted, then press [Enter].

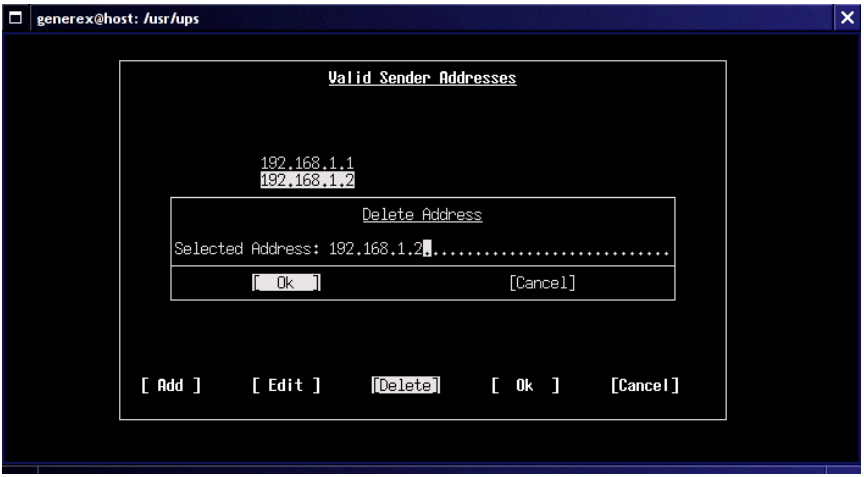


Figure 66 RCCMD UNIX Delete Sender

Confirm to delete the entry by selecting [Ok] with the [Tab] key and pressing [Enter], otherwise select [Cancel].

To leave the screen select either [Ok] or [Cancel] with the [Tab] key and press [Enter]. [Ok] means accept the list as displayed on the screen, [Cancel] means discard all changes made to the list.

Scan for Upsman/Upstcp:

This screen allows you to scan your network for Upsman/Upstcp servers. You may want to add the detected IP addresses to the “Access Control List”.

Note: **The options on this screen do not directly affect rccmd. However, the results of a network scan may be transferred to the “Access Control List”.**

Figure 67 RCCMD UNIX Sender Scan

lowest/highest IP:	On startup rccmd_conf tries to determine the hosts primary IP address. From this address a corresponding Class C network range is derived. These are the default boundaries for the network scan. If you want to scan another network or adjust the range, move to the desired entry (lowest and/or highest IP) using the [Tab] key and change the address as appropriate.
Port to Scan:	The port the scanner will try to connect to. The default is 5769, which is the default port of the Upsman/Upstcp server. If you have Upsman/Upstcp running on a different port you may want to switch this option accordingly.

To start the scan select [Scan] using the [Tab] key and press [Enter], otherwise select [Cancel].

Configure “Check Upsman/Upstcp”:

The Rccmd listener has the ability to check periodically if the Upsman/Upstcp servers configured in “Access Control List” are alive.

Note: **The “Check Upsman/Upstcp” feature is only available if there are any addresses configured in the “Access Control List”.**

If there are one or more entries in “Access Control List” the screen “Check Upsman Options” pops up.

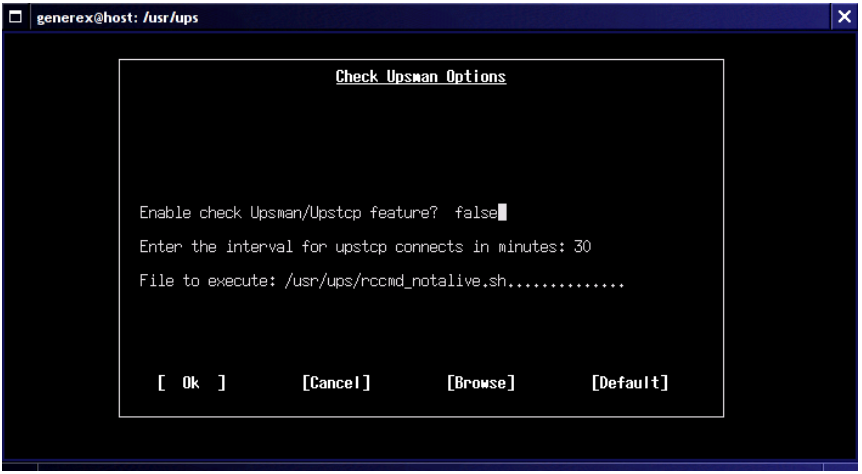


Figure 68 RCCMD UNIX Check Upsman

Use the [Tab] key to move through the option-fields and buttons.

Enable check Upsman/Upstcp feature: Possible values are “true” and “false”, “false” is the default. To change the value use the [↑] and [↓] keys.

Enter the interval for upstcp connects in minutes:

Interval to connect Upsman/Upstcp servers in minutes. Default is 30 minutes. To change overwrite the value in the options field.

File to execute: This file will be executed if rccmd is not able to connect one (or more) of the configured Upsman/Upstcp servers, asuming that either the host is down or the Upsman/Upstcp process is not running. Default is '/usr/ups/rccmd_notalive.sh'. You may change this value by overwriting the string in the options-field or by selecting a file in the file-browser. To invoke the file-browser hit the [Tab] key until the [Browse] button is highlighted, then press [Enter].

To reset all values to their defaults select the [Default] button by hitting the [Tab] key, then press [Enter].

To leave the Screen select either [Ok] or [Cancel] with the [Tab] key and press [Enter], [Ok] means accept all values as displayed on the screen, [Cancel] means discard all changes made to the screen and switch back to the previous state.

Configure “Logfile Options”:

The rccmd listener is able to write and maintain a logfile. It will log events such as startup and shutdown of the program, accepted and denied network connections and executed commands. Some parameters may be configured on this screen.

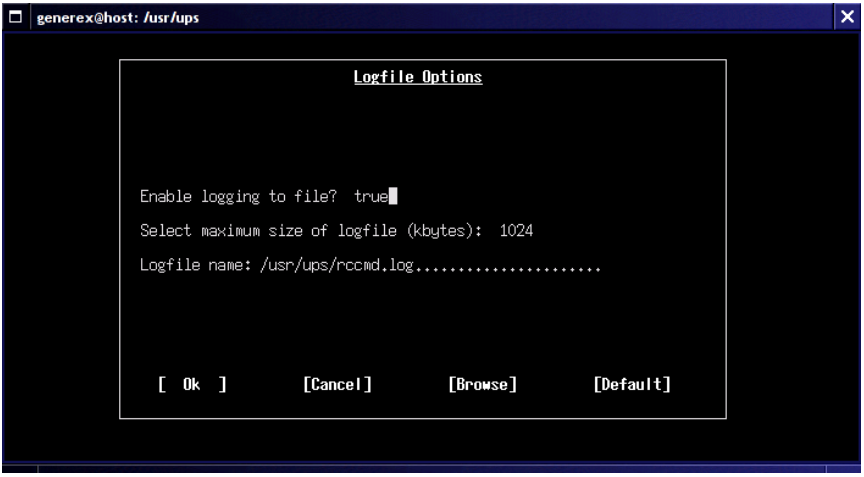


Figure 69 RCCMD UNIX Log File Options

Enable logging to file:	Possible values are “true” and “false”, “true” is the default. To change the value use the [↑] and [↓] keys.
Select maximum size of log file:	The log file will not gain larger than this size. If the size of the log file would exceed this limit rccmd will automatically shrink it by 10% before it continues write to the log. The file will be shrinked from the start, so older entries will be removed first. The default size is 1024 Kb. To change the value use the [↑] and [↓] keys. The special value '0' means the file will not be shrinked.
Log file name:	This option specifies the name and location of the logfile. The default is “/usr/ups/rccmd.log”. You may change this value by overwriting the string in the options-field or by selecting a file in the file-browser. To invoke the file-browser hit the [Tab]

key until the [Browse] button is highlighted, then press [Enter].

To reset all values to their defaults select the [Default] button by hitting the [Tab] key, then press [Enter].

To leave the Screen select either [Ok] or [Cancel] with the [Tab] key and press [Enter], [Ok] means accept all values as displayed on the screen, [Cancel] means discard all changes made to the screen and switch back to the previous state.

Configure “Shutdown Options”:

Figure 70 RCCMD UNIX Shutdown Options

File to execute: This file will be executed if rccmd receives the “SHUTDOWN” command from the network. Default is /usr/ups/rccmd_shutdown.sh. You may change this value by overwriting the string in the options-field or by selecting a file in the file-browser. To invoke the file-browser hit the [Tab] key until the [Browse] button is highlighted, then press [Enter].

To reset all values to their defaults select the [Default] button by hitting the [Tab] key, then press [Enter].

To leave the Screen select either [Ok] or [Cancel] with the [Tab] key and press [Enter], [Ok] means accept all values as displayed on the screen, [Cancel] means discard all changes made to the screen and switch back to the previous state.

Exit rccmd_conf:

In the main configuration menu “Rccmd Configuration” select either [Save] or [Exit] by hitting the [Tab] key until the desired button is highlighted and press [Enter]. [Save] means 'rccmd.cfg' will be written according to the actual values of the configuration screens, [Exit] will just exit the program, leaving 'rccmd.cfg' untouched.

The File Browser:

Some of the screens above use a small build-in file browser like this:

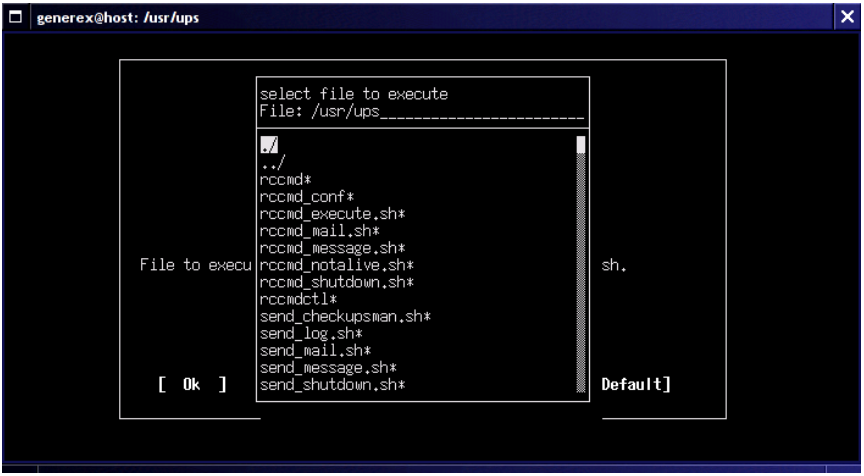


Figure 71 RCCMD UNIX File Browsing

The [↑] and [↓] keys may be used to move the list up and down. Pressing the [Enter] key will select the highlighted entry. If the selected entry is a directory the browser wil move into this directory and list its contents. As usual the double dot '..' means the parent directory. File types are indicated similar to the output of 'ls -F'. This means a '*' is appended for executables, '/' for directories, '@' for symbolic links and '=' for sockets.

UNIX RCCMD multiple sender configuration (V1 – V2):

In case the user wants to utilise more than one sender address the rccmd.sh has to be modified like this:

```
#! /bin/sh

# You may specify a sender IP to accept signals from,
# default is everyone.
SENDER="-a 10.55.52.82 -a 10.55.52.83 -a 10.55.52.84"

# You may change the port to listen on,
# default is 6003.
PORT=
```

```
# You must define a command to be executed upon
# receiving signal.
SCRIPT=/usr/ups/doshutdown.sh

# test -z $SENDER || SENDER="-a $SENDER"
test -z $PORT || PORT="-p $PORT"

# to start:
./rccmd -l $SENDER $PORT $SCRIPT
```

UNIX RCCMD multiple sender configuration (V3 and higher):

How to start several RCCMD sessions via different ports on UNIX?

Every RCCMD session needs an own TCP port, e. g.:

```
./rccmd –l –p 6003
./rccmd –l –p 6004
./rccmd –l –p 6005
```

Import into RC files:

Set an accordant amount of starting scripts and invoke them trough the old ones:

a) Create new starting scripts, copy 3 times the old script and rename them:

```
cp rccmdctl.sh rccmdctl-1.sh
cp rccmdctl.sh rccmdctl-2.sh
cp rccmdctl.sh rccmdctl-3.sh
```

b) Adjust the new scripts through the variable “RCCMDPORT”:

```
...
RCCMDPORT=6003
...
```

Adjust the old script, because it starts the new one, replace the start- and stop sector in the folder „rccmdctl“:

```
start)
/usr/ups/rccmdctl-1.sh start
/usr/ups/rccmdctl-2.sh start
/usr/ups/rccmdctl-3.sh start
;;

stop)
/usr/ups/rccmdctl-1.sh stop
/usr/ups/rccmdctl-2.sh stop
/usr/ups/rccmdctl-3.sh stop
;;
```

Attention:

Do not edit the scripts with a Windows editor, because the different word wrap of Windows/Unix would destroy them!

4.4 RCCMD Client as Relay Station

If you need to reach a bigger amount of receivers, it is required to define the CS121 as relay station. The receiver must be defined, if receiving a RCCMD signal, that it will start a script, which will send further RCCMD signals. The workstation is receiver and sender at the same time and thus an important connection in the UPS monitoring. The usage of a RCCMD client as relay station makes the monitoring of more than hundred RCCMD clients as easier as the configuration of the CS121 via web-browser. Furthermore the web-browser event configuration got a limit, so that it is required to use the relay function, if the amount of jobs is more than 50 per event at the CS121.

The following steps are required for the configuration of the relay function:

- Open the file “rccmd_shutdown.sh” with an editor.
- Add prior of the shutdown of the workstation (“shutdown –h now”) the relay calls, e. g. the call of the included “send_shutdown.sh”.
- Add the desired IP addresses or rather the DNS names:

```
./send_shutdown.sh -a 10.10.10.10 -a 10.10.10.11 -a 10.10.10.12
```

- Save the settings of the “rccmd_shutdown.sh”.

4.5 RCCMD with SSL for UNIX

The Secure Sockets Layer (SSL) protocol is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks.

Use your Web-browser to navigate to the address of your UPS Web-Manager. Click the “Network & Security” configuration button and enable the SSL network feature.

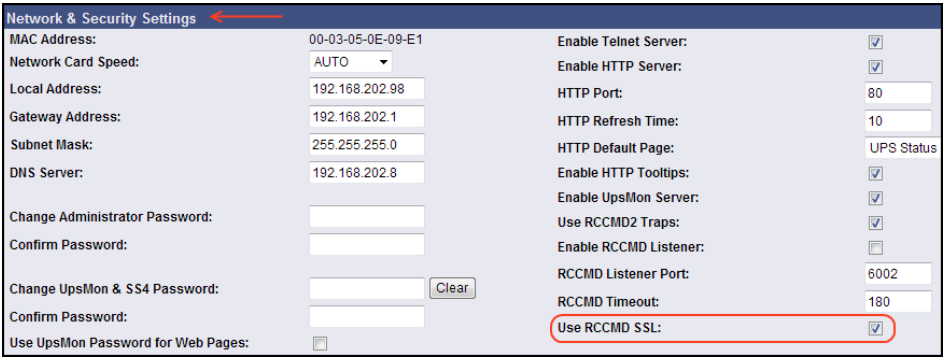


Figure 72 RCCMD SSL Settings

The SSL network feature requires correct time settings, so it is required to configure a timeserver. Click the „Timeserver“ configuration button and enter the address of at least one timeserver.

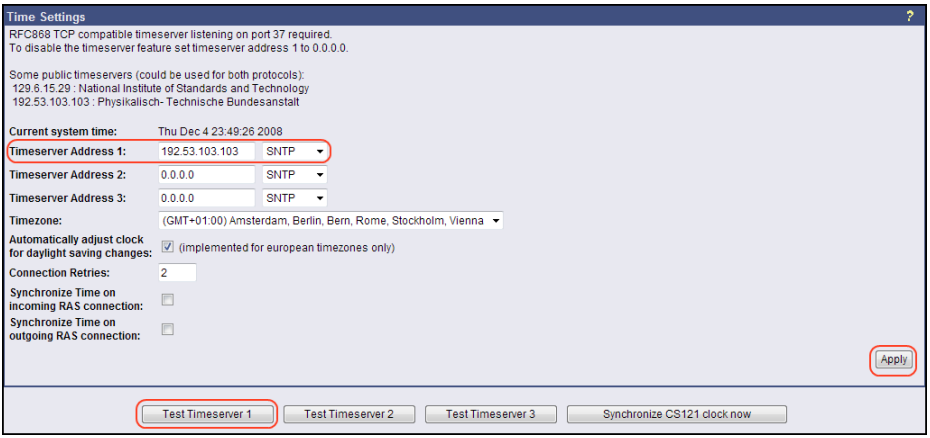


Figure 73 Timeserver Settings

Click the „Save Configuration“ button and the „Save, Exit & Reboot“ button to confirm your settings.

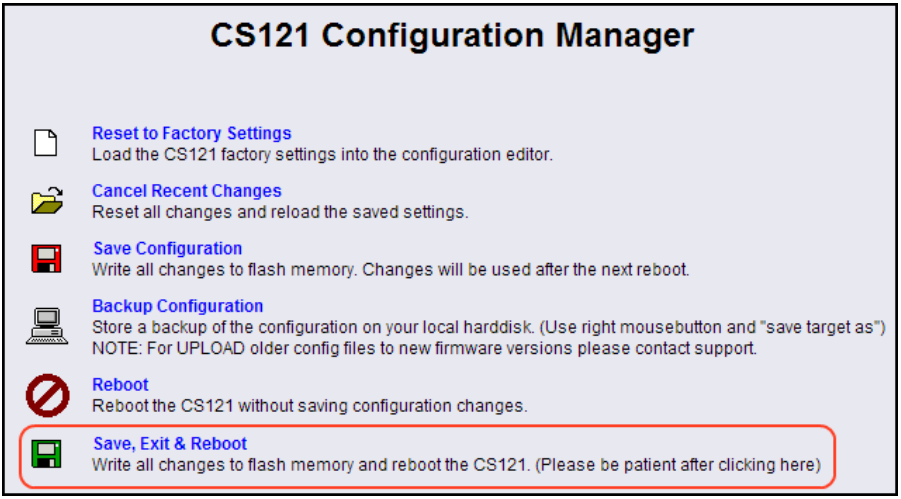

CS121 Configuration Manager
Reset to Factory Settings
Load the CS121 factory settings into the configuration editor.
Cancel Recent Changes
Reset all changes and reload the saved settings.
Save Configuration
Write all changes to flash memory. Changes will be used after the next reboot.
Backup Configuration
Store a backup of the configuration on your local harddisk. (Use right mousebutton and "save target as")
NOTE: For UPLOAD older config files to new firmware versions please contact support.
Reboot
Reboot the CS121 without saving configuration changes.
Save, Exit & Reboot
Write all changes to flash memory and reboot the CS121. (Please be patient after clicking here)

Figure 74 Settings Confirmation

Go to the RCCMD installation folder (e. g. /usr/ups) and start the RCCMD configuration:

```
/rccmdctl conf
```

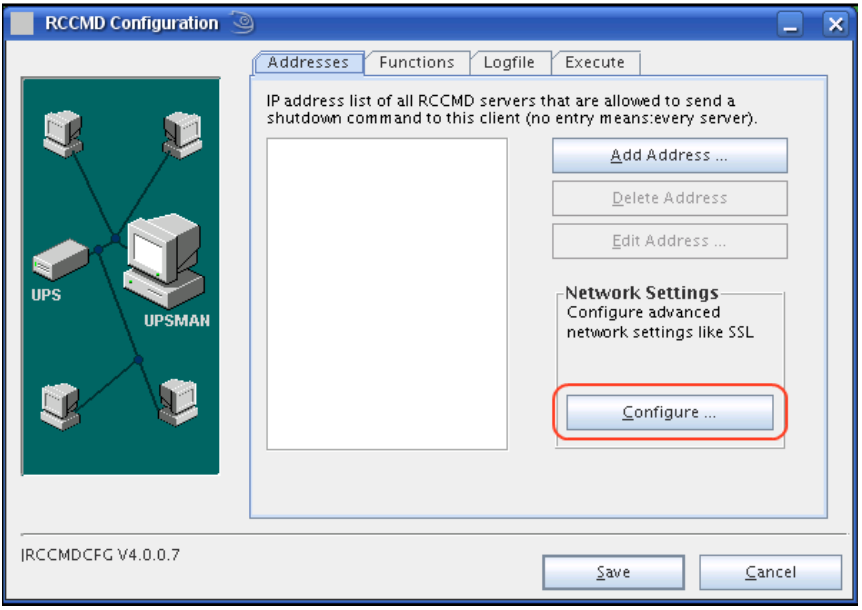


Figure 75 SSL Configuration

Enable the SSL network feature.

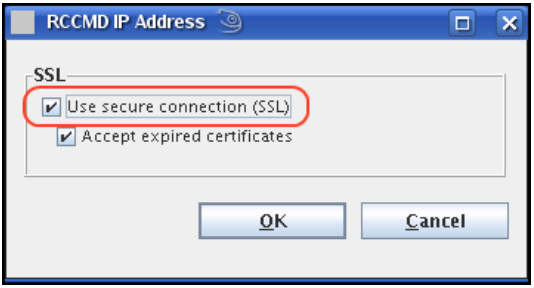


Figure 76 Advanced Network Settings

Alternative configuration with an text editor

You can set the desired configuration with an ASCII editor into the configuration data „rccmd.cfg“ manually.

```
# RCCMD Configuration (v2-default)

#

# Bind on Interface

# Defines on which interface we listen for incoming commands
```

```
# Default: 0.0.0.0 (All possible interfaces on this host)
#
ListenAddress=0.0.0.0
#
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
#
ListenPort=6003
#
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
#
ListenUDP=true
#
# Access Control List
# A list of valid sender addresses, only its members can connect
to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1
192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
#
AllowedAddresses=
#
# SSL: Use SSL
# Enables (true) or disables (false) SSL Connections
# Default: false
#
SSL=false
```

```
#
# SSL: Reject expired certificates
# Permits (false) or denies (true) connections with expired
cert's.
# Default: false
#
```

SSLRejectExpiredCert=false

The SSL configuration occurs via the following entries:

SSL=*true*

SSLRejectExpiredCert=false

During the installation you can merge the grafical configuration and create a narrated „rccmd.cfg“ at the same time, if you answer the following question:

```
This is NOT an ITANIUM (IA-64) system [Y/n]?:
```

with „n“.

4.5.1 RCCMD with own SSL certificates

In this chapter we will describe, how to use an own SSL certificate with RCCMD, e. g. OpenSSL (http://www.openssl.org):

Be your own CA

Using OpenSSL it is quite simple to become your own CA. Just run:

```
CA.pl –newca
```

Done! Just ensure, that you select a useful CN (common name)!

Create your RCCMD certificate

You need to create your certificate for RCCMD now. As it will use it for verification, it should contain the same useful common name (CN), that you selected for the CA. The private key must not be encrypted to let the RCCMD Client (service) start without trouble. Therefore we use the “–nodes” option and the “-newreq” command:

```
CA.pl –newreq -nodes
```

Sign with your CA:

```
CA.pl –sign
```

Now create an empty filed named “rccmd.pem“ and copy the cert information of *newcert.pem* (rccmd certificate), *newkey.pem* (private key) and *cacert.pem* (CA) into it. Please note, that the exact copying is required to use it without trouble!

Use your own RCCMD certificate

Do the following steps at the RCCMD Client and every sender (e. g. UPS Web Manager):

- Backup the existing “rccmd.pem”
- Replace the existing “rccmd.pem” with your own
- Restart the RCCMD Client
- Restart the RCCMD Sender

5. RCCMD on DEC VMS

The UPS-Management-Software CD contains the RCCMD software. The VMS RCCMD installation can be done by following the UNIX installation instructions in this manual, all of the steps are the same.

Note: **The VMS license is not part of the standard CD; It is to be ordered separately. It is not permitted to use the VMS version and its RCCMD modules without registered license.**

Prior of the installation you should verify that port 6003 is not in use. Check this with the command « netstat –an ». Ensure that there is no other process running or start the RCCMD module at another port address with the option –p for sending and receiving. Ensure too, that you will use this port for every command in the network. Please follow the instructions of the next chapter carefully. For further help you may use the user manual and the troubleshooting pages or contact your UPS software dealer.

Important: **The Alpha-Version is linked to OpenVMS 7.1. For OpenVMS 6.x use the Version 6.x in the following CD directory (ex. DKA200:[VMS.ALPHA.6X]).**

Installation procedure:

- Connect the workstation to the network.
- Login into the VMS System using SYSTEM login.
- Mount the CD-ROM device (if DKA200 is the device name of the CD-ROM):

$ MOUNT/OVERRIDE=IDENT DKA200: UPS UPS:

This is a system specific command. Use the VMS help pages for your system or ask the system operator, if you do not know, how to mount your input device.

- Start the VMS install procedure by: @SYS$UPDATE:VMSINSTAL
- or: @SYS$UPDATE:VMSINSTAL <device>
- e. g.: @SYS$UPDATE:VMSINSTAL RCCMD DKA200: [VMS.ALPHA]

VMSINSTAL is an interactive script, so just follow the installation instructions on the screen (all instructions are aditionally listed in the following subjects 5-11).

- Answer YES at the prompt: "* *Are you satisfied with the backup of your system disk [YES*]"
- Answer the prompt: "* *Where will the distribution volumes be mounted*:" with your correct input device name e. g.:

CDROM: *dka500: [VMS]* (your CDROM device and path [VMS], the device may be different on your system).

- Answer the prompt*:"* Enter installation options you wish to use [none]:"* by pressing RETURN
- At the prompt*:"Please mount the first volume of the set on MKA300:." "* Are you ready?"* please insert your tape (or disk or CDROM) and answer *"yes"*
- Enter the license key of your RCCMD version
- Enter the complete path of the target directory, e. g.: *dka100: [ups]*
- Answer the question *"Would you like to start the RCCMD module automatically on your system".*
- Exit the VMSINSTALL procedure by RETURN at the "*Product:" prompt and change to your target UPS directory (e. g.: set default dka100: [ups])
- Now install the RCCMD software in sending mode on your RCCMD server workstation. Your server workstation is the computer, which is connected to the UPS via the RS232 port.

DEC ALPHA CD Problems: If the CD could not be mounted or if you have problems to start the VMSINSTAL script on the DEC ALPHA hardware, please follow the instructions below:

- Copy the archive VMSA.ZIP (ALPHA directory) into a temporary directory on your system. COPY RCCMD.ZIP DKA100:[TEMP]

If you have not installed the ZIP utilities on your workstation already, you have to assign a system value: UNZIP==$DKA200:[VMS.ALPHA]UNZIP.EXE, where DKA200: is your CDROM device.

- Unpack your VMS UPS archive:

SET DEF DKA100:[TEMP] UNZIP RCCMD.ZIP

- Start the VMS installation routine: @SYS$UPDATE:VMSINSTAL RCCMD DKA100:[TEMP]

Configuration procedure:

After the installation there are 3 command files:

- RCCMDSTART.COM: RCCMD startup command file should be called in the VMS startup file
- RCCMD.COM: Command file to start RCCMD program itself, this should be configured to your requirements
- RCCMD_SHUTDOWN.COM: sample command file which could be called by RCCMD to shutdown VMS

Configure the RCCMD.COM command file by calling the RCCMD program with the following command: “rccmd –l” optional you can use “rccmd –l –a<IP address of the sender> -p <port (standard 6003)>”. After that you can start the RCCMD by caklling the command file RCCMDSTART.COM with “@rccmdstart”.

Check the process by calling “show system”. There should be a process with the name RCCMD.

The automatic startof the RCCMD should be initiated from the VMS startup file. You may use the enclosed script rccmdstart.com. Add a line to your startup file (prior to the exit command):

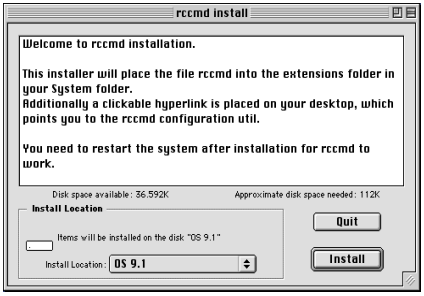
$ @your_disk:[your_path]rccmdstart.com (e. g.: $ @dka100:[ups]rccmdstart.com)

The UPS software will be started automatically after the next reboot.

6. RCCMD on MAC OS 9

The installation of RCCMD under MAC OS 9 is no longer supported, currently we support only RCCMD for MAC OS X 10.4 and higher. Following we describe the former MAC OS 9 RCCMD installation. The RCCMD installation automatically copies an alias ontop the desktop (rccmd configuration.url).

1.


rccmd install
Welcome to rccmd installation.
This installer will place the file rccmd into the extensions folder in your System folder.
Additionally a clickable hyperlink is placed on your desktop, which points you to the rccmd configuration util.
You need to restart the system after installation for rccmd to work.
Disk space available: 36.592K
Approximate disk space needed: 112K
Install Location
Items will be installed on the disk "OS 9.1"
Install Location: OS 9.1
Quit
Install

After the installation of the RCCMD archives , the following dialogue opens:

After restarting the computer, the RCCMD configuration tools can begin. In order to do this, please click on the alias "rccmd configuartion.url" A standard Web-browser (e.g. IE 5.x or Netscape Navigator 4.x) will start now.

Figure 77 Mac OS RCCMD Install Startup

2.

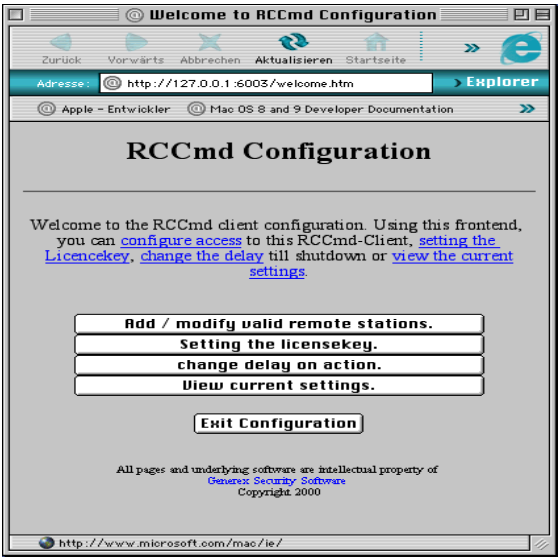
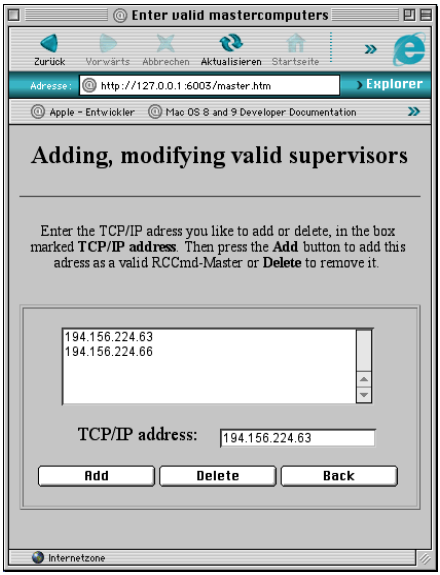


Figure 78 Mac OS RCCMD Configuration

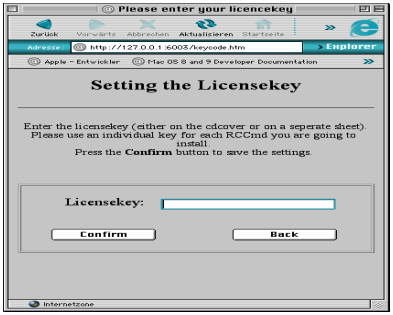
The following window opens

It is recommendable to execute the menue options from top down.



This option allows the entry of the IP addresses of the RCCMD sender, those workstations, which send the shutdown signals to the remote computers (RCCMD clients). The configuration of the RCCMD sender is executed from the UPSMAN configuration. Please also check the RCCMD Windows section of this manual. Please enter the IP address(es) of the RCCMD sender into the field TCP/IP address" and click onto "Add" in order to add the address to the list. Repeat this method if several RCCMD senders should be in the list. To delete, simply highlight the IP address of a RCCMD sender from the list and click the "Delete" Button.

Figure 79 Mac OS Add/ Modify Valid Remote Stations



Please enter the license key, which came with the copy of your CD or the separate purchased RCCMD license (additional license). Please confirm your entry by clicking on "Confirm" The "Back" button, will take the user back to the RCCMD main menue.

Figure 80 Mac OS Setting the License Key

Please note the license regulations regarding RCCMD sender and clients. The standard version of the MAC OS UPS-Management software can send RCCMD (send) signals to an unlimited number of RCCMD clients. Per license only one RCCMD client can be execute a shutdown. Please contact your UPS dealer, if you require additional RCCMD licenses or order at www.generex.de.

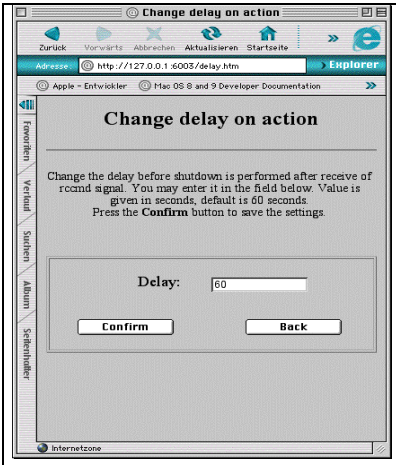


Figure 81 Mac OS Change Delay On Action

The menue "Change delay on action" allows the user to enter a delay in seconds, before the shutdown of the RCCMD client(s) is initiated and after a shutdown signal is received. The default is 60 seconds –using "Confirm" will configure your settings.

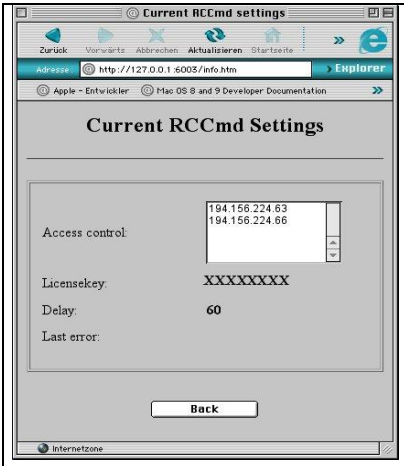


Figure 82 Mac OS View Current Settings

This window shows the user the current RCCMD settings. The access control field shows RCCMD sender, which have sending authority, the license key, the current delay in seconds from the "Delay on action" feature, followed by the last RCCMD error report. The Back" button will bring you back to the RCCMD main menu. Generally, RCCMD is started automatically after a successful installation. If this is not required. Please remove the corresponding system extension from the system extensions folder.

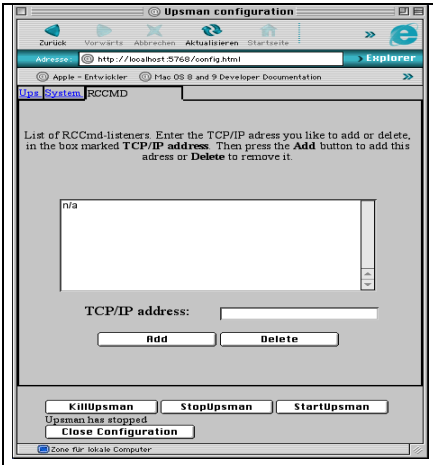


Figure 83 Mac OS Add RCCMD Receivers (RCCMD Clients)

Please start the alias „upsman configuration.url“, as described in the previous section, using your standard web-browser. The following dialogue opens:

Please enter the IP address(es) of the RCCMD clients in the field "TCP/IP address" and click "Add", in order to add the addresses to the list. Please repeat the method, if several IP addresses/RCCMD clients need to be added to the list. On the other hand, deleting an IP address is simply done by highlighting the corresponding address and clicking the "Delete" button. Please note the license regulations in the previous section "Setting the license key"

Equal to the UPSMAN Windows configuration, we recommend to limit the group/number of RCCMD receivers, because without an entry into the receiver list, all RCCMD receivers (clients) in the network will perform a shutdown (depending on license status), when a RCCMD sender signal is executed. The RCCMD configuration is now complete.

7. RCCMD on MAC OS 10.X

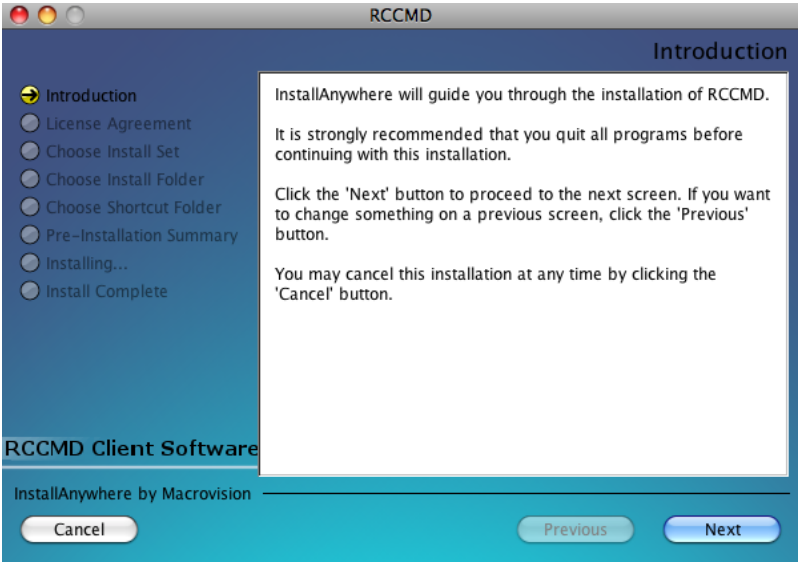

RCCMD
Introduction
Introduction
License Agreement
Choose Install Set
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...
Install Complete
InstallAnywhere will guide you through the installation of RCCMD.
It is strongly recommended that you quit all programs before continuing with this installation.
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.
You may cancel this installation at any time by clicking the 'Cancel' button.
RCCMD Client Software
InstallAnywhere by Macrovision
Cancel
Previous
Next

Figure 84 RCCMD Installation Welcome

You need a special license key for your RCCMD software. You can identify the key with the **"RX3"** in the first part of the license key. Most of the times you need to order the key separately.

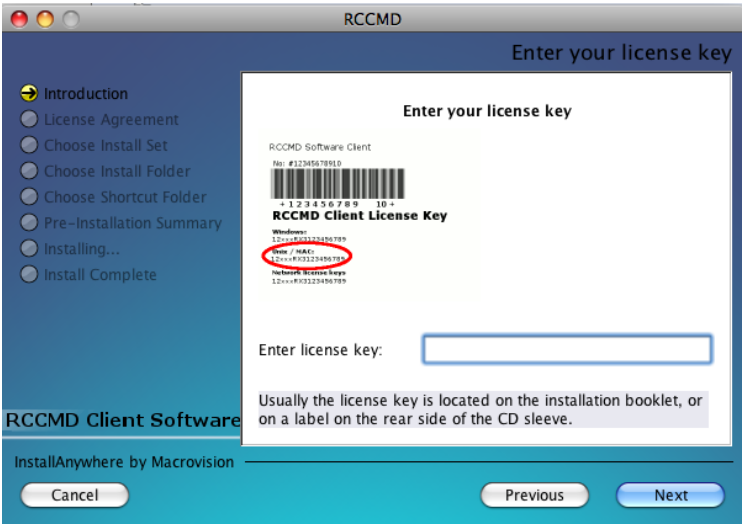


Figure 85 RCCMD Enter Your License Key

Select a destination volume to install the RCCMD software.

Figure 86 RCCMD Pre-Installation-Overview

Add the IP address of the RCCMD server, which is allowed to send a shutdown to this client.

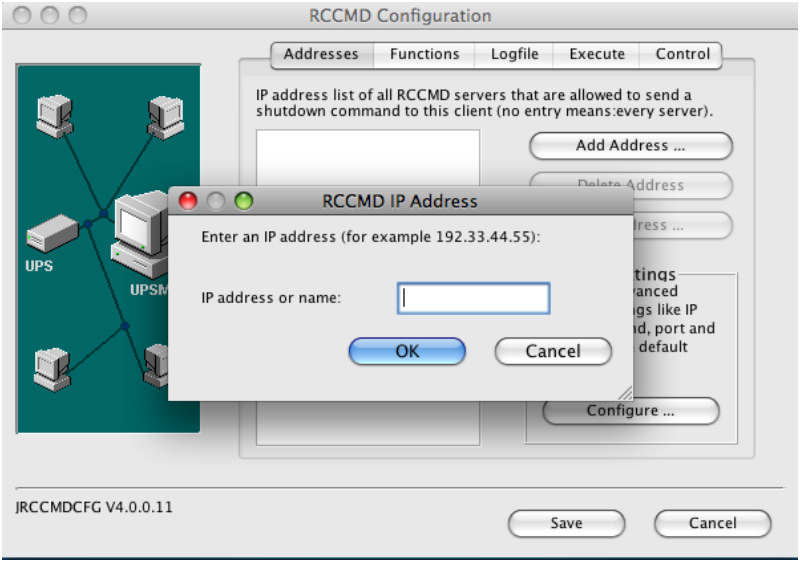


Figure 87 RCCMD IP Address Window

Attention:

If you do not enter an address, then every server has the permission to send a shutdown command. If more than one CS121 or rather UPSMAN is existent, thus a redundancy situation, you need to enter more than one address as authorized sender.

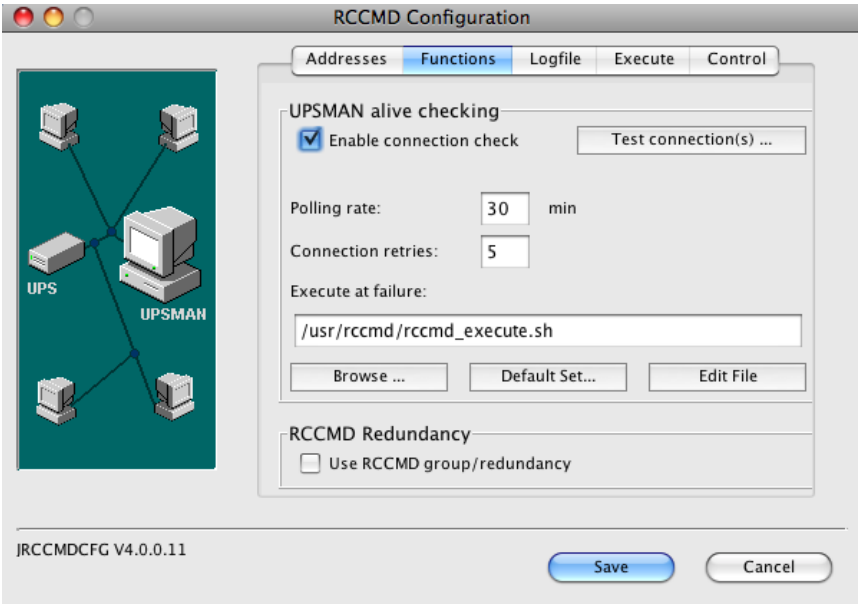


Figure 88 RCCMD Configuration Window „Functions“

If you want to use the UPSMAN alive checking (recommended), check the “Enable connection check” box. Alive check is a signal, send out to the UPSMAN or CS121 on port 5769 to check if the UPSMAN has still UPS data – or not. If this fails, the scriptfile alive.bat will be executed which causes a messagbox coming up. The polling rate (default 30 min.) defines the polling of the UPSMAN service, connect retries (default 5) means after 5 unsuccessful connection tries an alarm will be triggered.

If you click the “Test connection(s)…” button, the UPSMAN alive checking of the entered IP addresses will start (port 5769 will be tested).

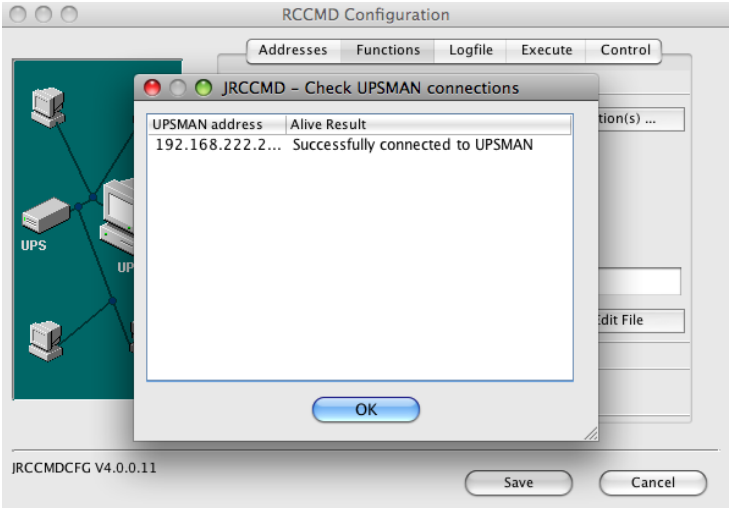


Figure 89 RCCMD Check UPSMAN Connections

If you click the „Browse...“ button, you will get a selection of the default batch files.

If you click the „Default setting“ button, you will get back to the default batchfile (alive.bat).

At the failure of the UPSMAN alive checking, you can define an executing file or edit the default file “alive.bat”.

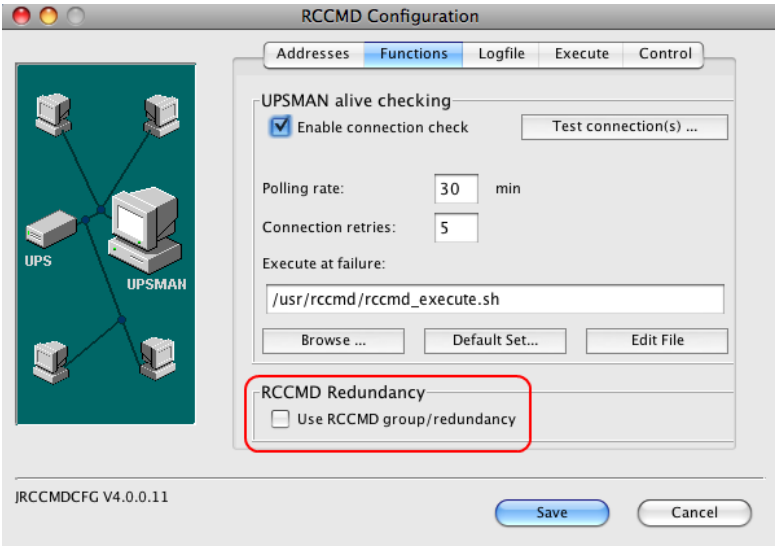


Figure 90 RCCMD Redundancy

At UPS installation RCCMD offers a **redundancy** management functionality as follows:

Every UPS must be equipped with a CS121 or UPSMAN software computer. When ticking the box “use RCCMD group/redundancy” – you are guided to a menue where you can choose which CS121 /UPSMAN are supplying this RCCMD client. E. g. if 4 CS121/UPSMAN are installed into 4 UPS – than each may send a shutdown signal to this RCCMD client.

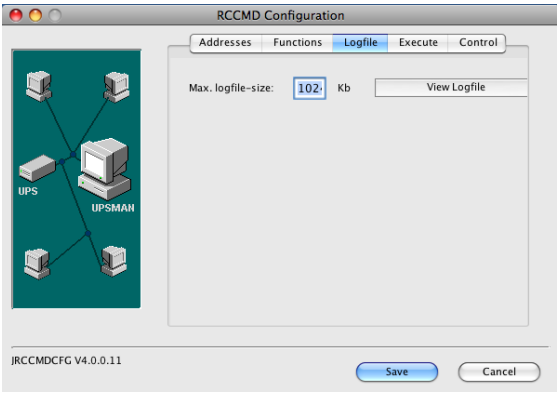


Figure 91 RCCMD Configuration Window „Logfile“

You can configure the log file size and edit the executing bat files in this installation window.

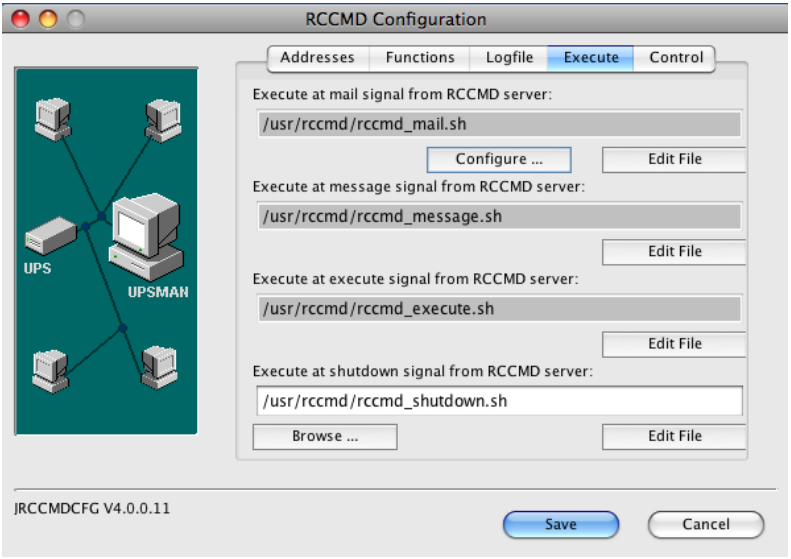


Figure 92 RCCMD ConfigurationWindow „Execute“

If you click the „Configure...“ button, you will be able to enter the mail settings and to use the mail function of RCCMD.

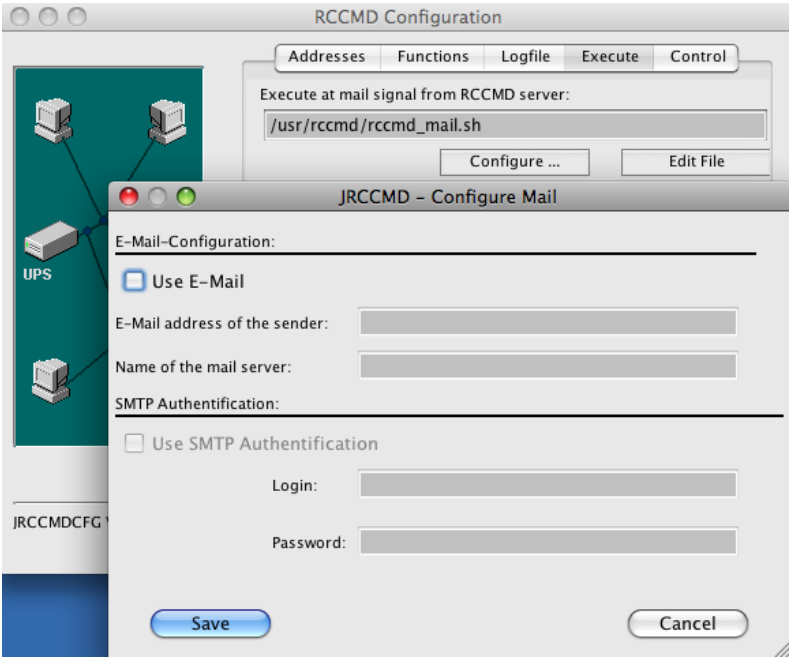


Figure 93 RCCMD E-Mail-Configuration

Click the „Control“ button to get into the folowing screen:

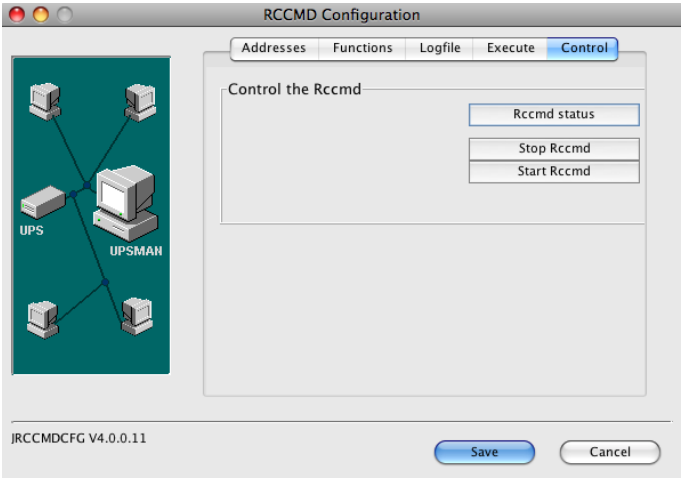


Figure 94 RCCMD Control

8. RCCMD on Citrix XEN Server

The RCCMD Software for Citrix XEN Server is a Linux based TCP client for receiving shutdown calls from UPSMAN software (any vendor), CS121 (any vendor) or other RCCMD licensed applications like SNMP adapters etc. from other vendors.

RCCMD for XEN Server runs on GNU Linux 2.6.18 or higher, which is the basis of the 2008 XEN Serverplatform.

For installing RCCMD please refer to the user manual of RCCMD for UNIX, following we describe some special aspects which are only applicable to XEN Server.

Installation:

Since the XEN Server does not offer any graphical interface, the download of RCCMD client for XEN Server from the GENEREX Website or other sites is not easy – unless you have extra tools installed like commandline browsers like Wget.

Additionally, by default, there is no FTP server active on XEN Server, so a transfer of a downloaded RCCMD package is also blocked. For this reason we recommend to use a local interface on your XEN Server like CD ROM Driver or, USB stick.

- Download RCCMD for XEN Server from the GENEREX Website – using your original RCCMD licensekey (not older than 2 years !) and extract the TAR file. Copy the files on a CD-R and insert this CD now into your XEN Server CD drive. Alternativly use UPSMAN CD ROM Version 5.48 or higher.

- Login as root and mount the CD ROM on the XEN Server:
  Enter: “mount /dev/cdrom /media” – Since it’s a CD ROM in your driver, the system will respond “mount: block device /dev/cdrom is write protected, mounting read-only”

- Change to the CD ROM by : “cd /media” – by “ls” you can see the files on the CD, change now to the folder UNIX (UPSMAN CD ROM) or “generex” until you find the installationprogramm “install”.

- Start now the installation by entering : “./install” and follow the instructions on the screen – from here the installation is identical to any other RCCMD installation for UNIX.

- After the installation is finished, a new process will be running on your XEN Server : “:/rccmd –l” which means the system is ready now.
  ATTENTION: XEN Server has per default a firewall active, which does not allow to send from remote RCCMD signals. To open this firewall you have to edit the file “iptables” (/etc/sysconfig #)

Firewall Configuration :

Add the following lines to */etc/sysconfig/iptables* **before** the last *REJECT* rule.

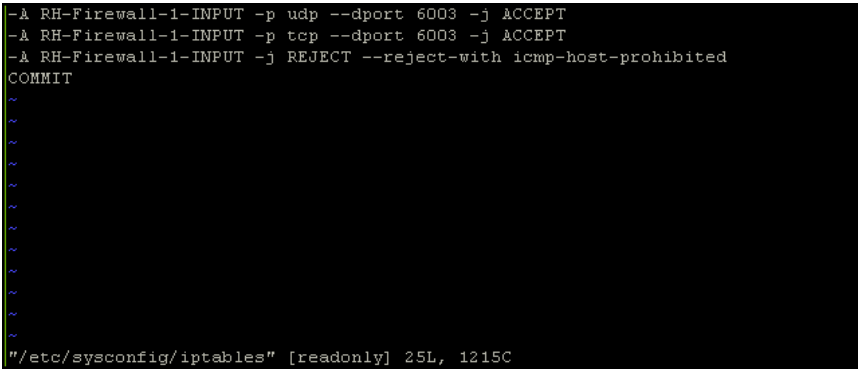

-A RH-Firewall-1-INPUT -p udp --dport 6003 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp --dport 6003 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
"/etc/sysconfig/iptables" [readonly] 25L, 1215C

Figure 95 Firewall Configuration

Restart the iptables using */etc/init.d/iptables restart* .

RCCMD is now listening and will start the file “shutdown.sh” on your XEN Server when any CS121 or UPSMAN transmit a RCCMD shutdown call. This file shutdown.sh makes an “init 0” shutdown on your XEN Server, edit this file, if you want to use a different shutdown procedure.

9. RCCMD on VMWare ESX Server 3.5.x

The RCCMD Software for VMWare ESX Server is a Linux based TCP client for receiving shutdown calls from UPSMAN software (any vendor), CS121 (any vendor) or other RCCMD licensed applications like SNMP adapters etc. from other vendors.

RCCMD for ESX Server runs on GNU Linux 2.6.18 or higher, which is the basis of the 2008 ESX 3.5.x Serverplatform.

For installing RCCMD please refer to the user manual of RCCMD for UNIX, following we describe some special aspects which are only applicable to ESX Server.

Installation:

Since the ESX Server does not offer any graphical interface, the download of RCCMD client for ESX Server from the GENEREX Website or other sites is not easy – unless you have extra tools installed like commandline browsers like Wget.

Additionally, by default, there is no FTP server active on ESX Server, so a transfer of a downloaded RCCMD package may be blocked. For this reason we recommend to use a local interface on your ESX Server like CD ROM Driver or USB stick.

- Download RCCMD for ESX Server from the GENEREX Website – using your original RCCMD licensekey (not older than 2 years !) and extract the TAR file.

Copy the files on a CD-R and insert this CD now into your ESX Server CD drive. Alternativly use UPSMAN CD ROM Version 5.48 or higher.

- Login as root and mount the CD ROM on the ESX Server:
  Enter: “mount /dev/cdrom ”
- Change to the CD ROM by : “cd /mnt/cdrom” – by “ls” you can see the files on the CD, change now to the folder UNIX (UPSMAN CD ROM) or “generex” until you find the installationprogramm “install”.

- Start now the installation by entering : “./install” and follow the instructions on the screen – from here the installation is identical to any other RCCMD installation for UNIX.

- After the installation is finished, a new process will be running on your ESX Server : “:/rccmd –l” which means the system is ready now.
  ATTENTION: ESX Server has per default a firewall active, which does not allow to send from remote RCCMD signals.

Firewall Configuration :

The following firewall configuration of the ESX Server is required to receive RCCMD signals:

```
esxcfg-firewall –o 6003,tcp,in,RCCMD
```

Restart the firewall service to apply your settings:

```
service firewall restart
```

RCCMD is now listening and will start the file “shutdown.sh” on your ESX Server when any CS121 or UPSMAN transmit a RCCMD shutdown call. This file shutdown.sh makes an “init0” shutdown on your ESX Server, edit this file, if you want to use a different shutdown procedure.

10. RCCMD on VMWare ESXi Server 4.0.x

The RCCMD Software for VMWare ESXi Server is a Linux based TCP client for receiving shutdown calls from UPSMAN software (any vendor), CS121 (any vendor) or other RCCMD licensed applications like SNMP adapters etc. from other vendors.

The VMWare provides the vSphere Management Assistant (vMA) 4.0 as appliance:

http://www.vmware.com/support/developer/vima/vima40/vma40relnotes.html

This vMA provides a management interface withal the ESXi server can be controlled via script.

It is possible to install RCCMD onto the vMA, because of the existing Linux Red Hat distribution there. The RCCMD installer detects automatically, that the installation will be performed onto a VMWare appliance and will install the accordant adjusted files.

The following conditions are required for the installation:

- A host is running onto the ESXi.
- A installed and configured vMA is existing, tip: vma_40_guide.pdf, page 13ff http://www.vmware.com/support/developer/vima/vima40/doc/vma_40_guide.pdf
- A vShpere-Client.
- A SCP client for the transfer of the RCCMD installer onto the vMA.

ESXi Host Configuration

RCCMD will execute the shutdown onto the ESXi host. Every host can be configured for the secure shutdown of its guest systems via the vSphere Client, but it is required to install the VMWare tools onto them.

Select into the vSphere Client your host (1), click at “configuration” (2) and tag “VMware starting/shutdown” (3). Now cklick the vMA button (4) and then “Properties” (5).

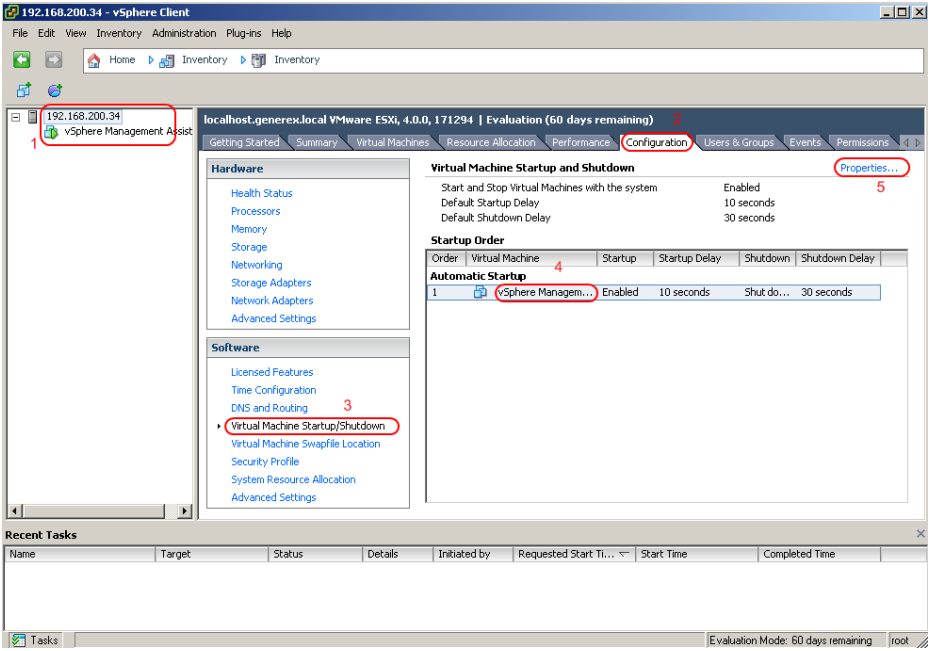


Figure 96 vSphere Client Configuration

Select into the properties dialog the vMA and set its values to 10 seconds start delay and 30 seconds shutdown delay.

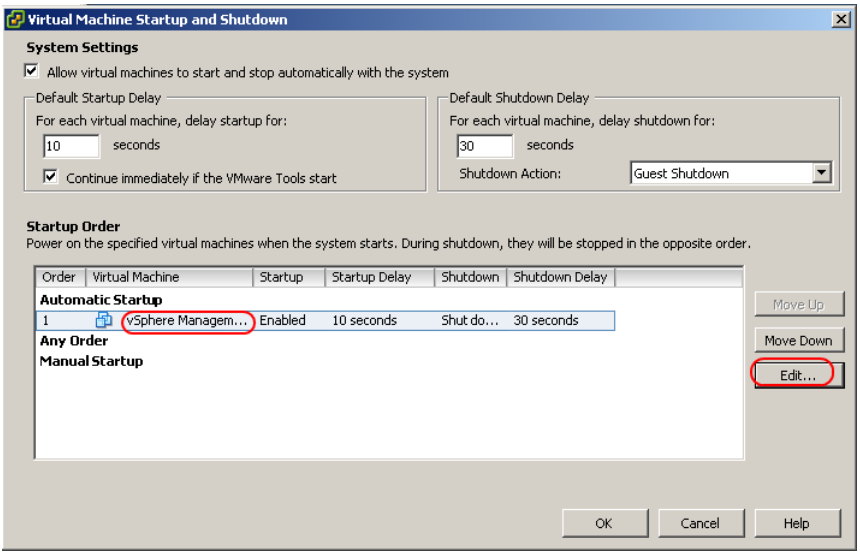


Figure 97 vSphere Client Auto-Start Configuration

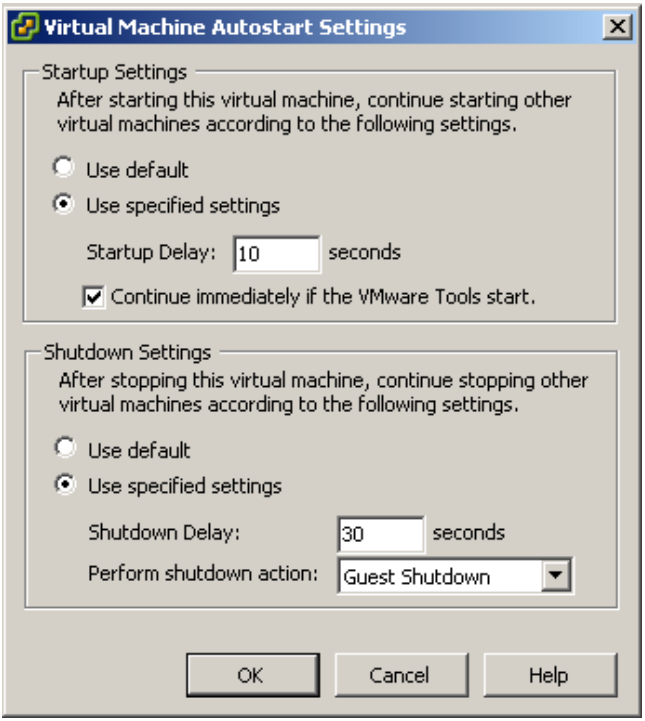


Figure 98 vSphere Client Auto-Start Delay

The further times of delay for the VMWares, who should be shut down via the host, can differ and should be arranged individually. Therefore the duration of the shutdown will increase accordingly.

Firewall Configuration

RCCMD requires port 6003 (TCP and UDP) for incoming IP packages. Please configure the firewall accordingly:

```
sudo system-config-securitylevel-tui
```

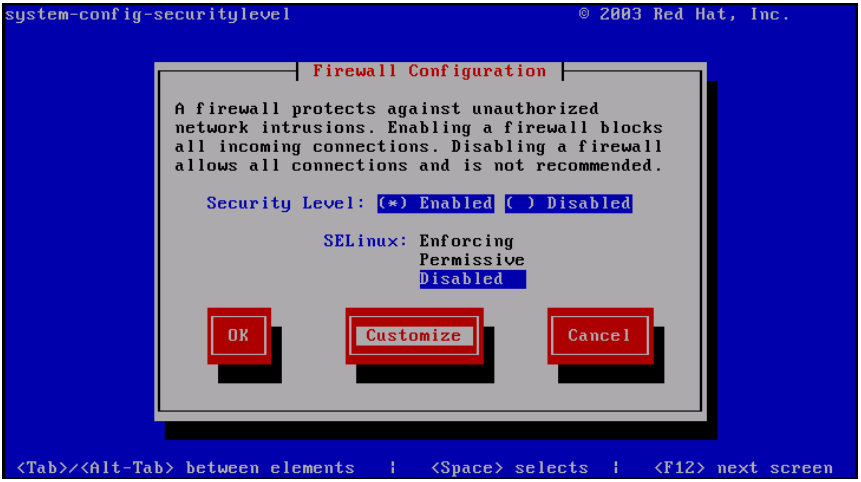

system-config-securitylevel
© 2003 Red Hat, Inc.
Firewall Configuration
A firewall protects against unauthorized network intrusions. Enabling a firewall blocks all incoming connections. Disabling a firewall allows all connections and is not recommended.
Security Level: (*) Enabled ( ) Disabled
SELinux: Enforcing
Permissive
Disabled
OK
Customize
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 99 Firewall Configuration

Click the „Customize“ button and complete the line „Other ports“ with 6003:tcp.

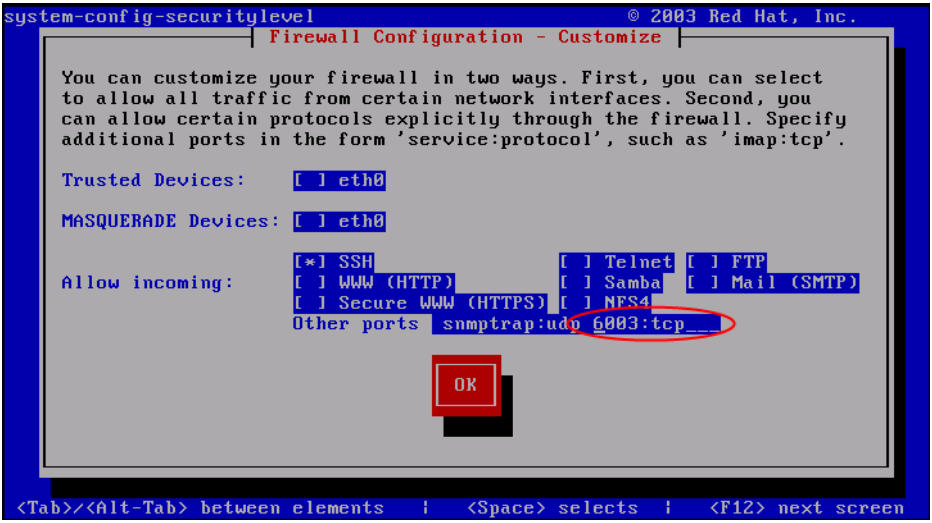

system-config-securitylevel
© 2003 Red Hat, Inc.
Firewall Configuration - Customize
You can customize your firewall in two ways. First, you can select to allow all traffic from certain network interfaces. Second, you can allow certain protocols explicitly through the firewall. Specify additional ports in the form 'service:protocol', such as 'imap:tcp'.
Trusted Devices: [ ] eth0
MASQUERADE Devices: [ ] eth0
Allow incoming: [*] SSH [ ] Telnet [ ] FTP
[ ] WWW (HTTP) [ ] Samba [ ] Mail (SMTP)
[ ] Secure WWW (HTTPS) [ ] NFS4
Other ports snmptrap:udp 6003:tcp
OK
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 100 Firewall Port Configuration

Restart the iptables as follows:

```
sudo etc/init.d/iptables restart
```

Check via the command `iptables –L`, if the accordant port 6003 is open.

RCCMD Installation

Copy the file RCCMDinst.tar via the SCP client (SFTP) onto the vMA. Extract the tar file as follows:

```
tar –xvf RCCMDinst.tar
```

The following installation oppurtunities are into the file „installer.properties“ at hand:

- Silent - It is required to remove the hash mark prior of the variable `INSTALLER_UI=silent`. Please note that it is required to set the server name or rather its IP address (“`ESXi_host=“server name“`).

- Console - If you want to activate the console installation, it is required to remove the hash mark prior of the variable `INSTALLER_UI=console` and to set the word console instead of silent. This is the interactive installation of RCCMD onto the console. Please execute the “installRCCMD.bin” as root.

RCCMD Configuration

All hosts, for which the vMA is registered, can be shut down through this installation of RCCMD.

It is required to edit the file rccmd_shutdown.sh (default folder `/usr/rccmd`). By the appeal of *upsVIShutdown.pl* it is essential to quote the hosts separately with a blank.

The host, where the vMA is running, has to be located in last place.

The configuration of RCCMD is achievable into the file rcmd.cfg (default folder `/usr/rccmd`).

11. RCCMD AS400-Client

RCCMD for AS 400 an iSeries is not described in this manual, but has identical functions as any other RCCMD. RCCMD for AS 400 comes with a separate user manual with the product.

Download AS400 RCCMD Manual

Appendix

A OpenSSL

"This product includes software developed by the OpenSSL Project for use

in the OpenSSL Toolkit (http://www.openssl.org/).

B Syntax for the switching of the outputs

Set the RCCMD client at port 6002 to “on”, define the CS121 AUX ports as outputs and restart the CS121. Install the RCCMD Windows Wizard and open a DOS box. The following is a syntax example with the IP address 192.168.202.165:

```
C:\RCCMD\
```

```
rccmd -s -a 192.168.202.165 -p 6002 -se "EXECUTE |AUX|1|1"
```

ATTENTION! The blank after the “Execute” is important!

Common syntax for the switching of AUX ports:

```
|AUX|1,0  Port1, set to low
|AUX|1,1  Port1, set to high
|AUX|2,0  Port2, set to low
|AUX|2,1  Port2, set to high
|AUX|3,0  Port3, set to low
|AUX|3,1  Port3, set to high
|AUX|4,0  Port4, set to low
|AUX|4,1  Port4, set to high
```

```
Syntax for the switching of the outputs of the SiteManager:
```

```
C:\RCCMD\rccmd -s -a 192.168.222.238 -p 6002 -se "EXECUTE
|UPSCMD|20000|1,1"
```

ATTENTION! The blank after the “Execute” is important!

Common syntax for the switching of the outputs of the SiteManager:

```
|UPSCMD|20000|1,0  output 1 to low
|UPSCMD|20000|1,1  output 1 to high
|UPSCMD|20000|2,0  output 2 to low
|UPSCMD|20000|2,1  output 2 to high
|UPSCMD|20000|3,0  output 3 to low
|UPSCMD|20000|3,1  output 3 to high
|UPSCMD|20000|4,0  output 4 to low
|UPSCMD|20000|4,1  output 4 to high
|UPSCMD|20000|5,0  output 5 to low
|UPSCMD|20000|5,1  output 5 to high
```

```
|UPSCMD|20000|6,0  output 6 to low
|UPSCMD|20000|6,1  output 6 to high
|UPSCMD|20000|7,0  output 7 to low
|UPSCMD|20000|7,1  output 7 to high

|UPSCMD|20000|8,0  output 8 to low
|UPSCMD|20000|8,1  output 8 to high
```

C Know How Pool

SuSE 8.1 or older Linux versions

If you are using a SuSE 8.1 or an older Linux version, it is required to select the OS „XEN-Server“ during the interactive RCCMD installation!

D Figures

Figure 1 RCCMD and UPSMAN in a network environment 6

Figure 2 Introduction 7

Figure 3 License Key Entry 8

Figure 4 License Agreement 9

Figure 5 Install Folder Selection 9

Figure 6 Shortcut Folder Selection 10

Figure 7 Summary 10

Figure 8 Client Installation 11

Figure 9 Add IP-Address Window 11

Figure 10 Advanced Network Settings 12

Figure 11 UPSMAN Alive Checking / Redundancy Window 12

Figure 12 Client Check Connection Batch File Window 13

Figure 13 Check UPSMAN Connections Window 14

Figure 14 Configure / Edit Bat Files 14

Figure 15 RCCMD Log File 15

Figure 16 RCCMD Shutdown Sequence Configuration 15

Figure 17 Content of the “installer.properties” 17

Figure 18 Client Installation successful Window 19

Figure 19 Enter your License Key 20
Figure 20 RCCMD Setup Type 21
Figure 21 Client Installation Window 21
Figure 22 RCCMD Properties Window 22
Figure 23 RCCMD Properties Log On Window 23
Figure 24 RCCMD Properties Password Confirmation 23
Figure 25 Select User Window 23
Figure 26 Selection of the Object Name 24
Figure 27 Administrator Selection 24
Figure 28 Administrator Password Confirmation 25
Figure 29 Service Right Info Window 25
Figure 30 Client Installation RCCMD Redundancy 26
Figure 31 Client Installation RCCMD Redundancy Configuration 27
Figure 32 Example: Batch File RCCMD act as Relay Station 28
Figure 33 RCCMD Client Shutdown Configuration 29
Figure 34 RCCMD Shutdown Relay 29
Figure 35 RCCMD Configuration IP Address Range 30
Figure 36 RCCMD Shutdown Relay Removal 30
Figure 37 RCCMD SSL Settings 33
Figure 38 Timeserver Settings 33
Figure 39 Settings Confirmation 34
Figure 40 SSL Configuration 34
Figure 41 Advanced Network Settings 35
Figure 42 RCCMD Console Test 38
Figure 43 RCCMD Alive Check via Command Line 38
Figure 44 UPSMAN Alive Check Window 39
Figure 45 RCCMD Console -? 39
Figure 46 Installation – Introduction 44
Figure 47 Installation – License Key 45

Figure 48 Installation – Choose Install Folder 45
Figure 49 Installation – RCCMD Messages 46
Figure 50 Installation – Pre-Installation Summary 46
Figure 51 Configuration – RCMD Sender IP Address 47
Figure 52 Configuration – RCMD Functions 47
Figure 53 Configuration – RCMD Redundancy 48
Figure 54 Configuration – RCMD Log File 49
Figure 55 Configuration – RCMD Execute 49
Figure 56 Configuration – RCMD E-Mail Configuration 50
Figure 57 Configuration – RCMD Control 50
Figure 58 Content of the “installer.properties” 51
Figure 59 Making the Configuration File 55
Figure 60 RCCMD Configuration Menu UNIX 55
Figure 61 RCCMD UNIX Network Options 56
Figure 62 RCCMD UNIX Add Sender 58
Figure 63 RCCMD UNIX Sender Example 58
Figure 64 RCCMD UNIX Sender Overview 59
Figure 65 RCCMD UNIX Edit Sender 59
Figure 66 RCCMD UNIX Delete Sender 60
Figure 67 RCCMD UNIX Sender Scan 61
Figure 68 RCCMD UNIX Check Upsman 62
Figure 69 RCCMD UNIX Log File Options 63
Figure 70 RCCMD UNIX Shutdown Options 64
Figure 71 RCCMD UNIX File Browsing 65
Figure 72 RCCMD SSL Settings 68
Figure 73 Timeserver Settings 68
Figure 74 Settings Confirmation 68
Figure 75 SSL Configuration 69
Figure 76 Advanced Network Settings 69

Figure 77 Mac OS RCCMD Install Startup 75
Figure 78 Mac OS RCCMD Configuration 75
Figure 79 Mac OS Add/ Modify Valid Remote Stations 76
Figure 80 Mac OS Setting the License Key 76
Figure 81 Mac OS Change Delay On Action 77
Figure 82 Mac OS View Current Settings 77
Figure 83 Mac OS Add RCCMD Receivers (RCCMD Clients) 78
Figure 84 RCCMD Installation Welcome 79
Figure 85 RCCMD Enter Your License Key 79
Figure 86 RCCMD Pre-Installation-Overview 80
Figure 87 RCCMD IP Address Window 80
Figure 88 RCCMD Configuration Window „Functions“ 81
Figure 89 RCCMD Check UPSMAN Connections 82
Figure 90 RCCMD Redundancy 82
Figure 91 RCCMD Configuration Window „Logfile“ 83
Figure 92 RCCMD ConfigurationWindow „Execute“ 83
Figure 93 RCCMD E-Mail-Configuration 84
Figure 94 RCCMD Control 84
Figure 95 Firewall Configuration 86
Figure 96 vSphere Client Configuration 88
Figure 97 vSphere Client Auto-Start Configuration 89
Figure 98 vSphere Client Auto-Start Delay 89
Figure 99 Firewall Configuration 90
Figure 100 Firewall Port Configuration 91